(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月18 日 (18.08.2005)

PCT

(10) 国際公開番号
WO 2005/076140 A1

(51) 国際特許分類[7]: G06F 12/14, G06K 17/00, G09C 1/00

(21) 国際出願番号: PCT/JP2005/001398

(22) 国際出願日: 2005 年2 月1 日 (01.02.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-026850 2004 年2 月3 日 (03.02.2004) JP
特願2004-125196 2004 年4 月21 日 (21.04.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 中野 稔久 (NAKANO, Toshihisa). 大森 基司 (OHMORI, Motoji). 横田 薫 (YOKOTA, Kaoru). 原田 俊治 (HARADA, Shunji). 井藤 好克 (ITO, Yoshikatsu). 藤村 一哉 (FUJIMURA, Kazuya). 高橋 潤 (TAKAHASHI, Jun).

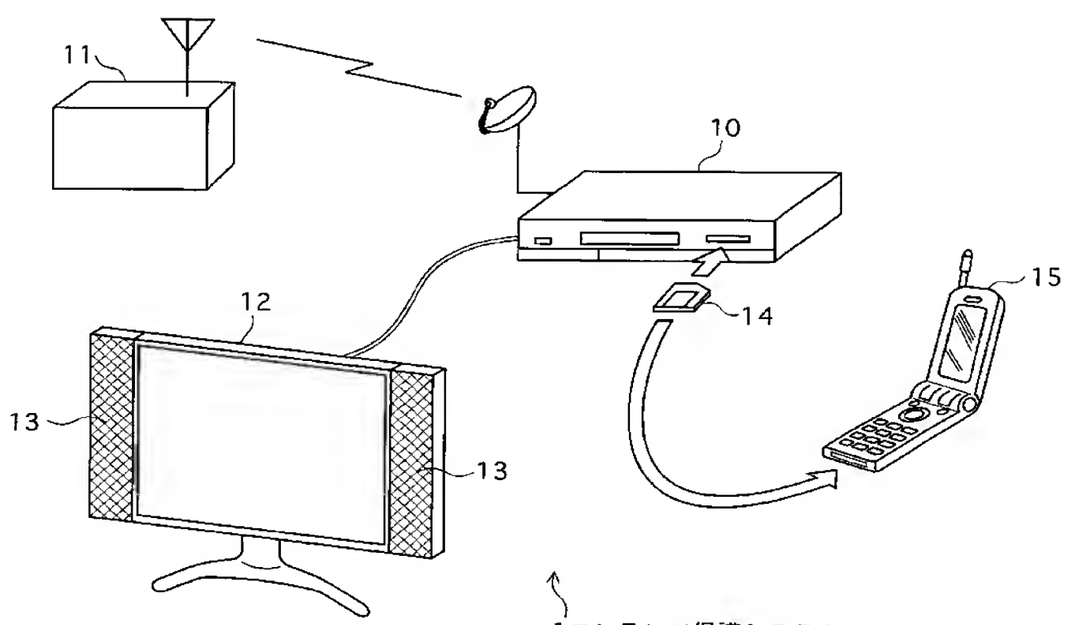
(74) 代理人: 中島 司朗, 外(NAKAJIMA, Shiro et al.); 〒5310072 大阪府大阪市北区豊崎三丁目２番１号淀川５番館６Ｆ Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,

[続葉有]

(54) Title: RECORDING/REPRODUCTION DEVICE AND CONTENT PROTECTION SYSTEM

(54) 発明の名称: 記録再生装置及びコンテンツ保護システム



WO 2005/076140 A1

1- CONTENT PROTECTION SYSTEM

(57) Abstract: A recording/reproduction device (10) receives a content broadcast from a content supply device (11). The recording/reproduction device (10) encrypts the received content by using a device key and generates a first encrypted content. The recording/reproduction device (10) decrypts the first encrypted content generated, and generates a content. The recording/reproduction device (10) subjects the generated content to an image conversion so as to generate a converted content and encrypts the generated converted content by using a medium key so as to generate a second encrypted content. The recording/reproduction device (10) writes the second encrypted content, the medium key, and the device key into a portable medium (14). When the portable medium (14) is inserted into a mobile information terminal (15), the mobile information terminal (15) decrypts the second encrypted content by the medium key and reproduces it.

(57) 要約: 記録再生装置１０は、コンテンツ供給装置１１から放送されるコンテンツを受信する。記録再生装置１０は、受信したコンテンツを装置鍵を用いて暗号化し、第１暗号化コンテンツを生成する。記録再生装置１０は、生成した第１暗号化コンテンツを復号して、コンテンツを生成する。記録再生装

[続葉有]

LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 補正書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

置１０は、生成したコンテンツに画像変換を施して、変換コンテンツを生成し、生成した変換コンテンツを媒体鍵で暗号化し、第２暗号化コンテンツを生成する。記録再生装置１０は、第２暗号化コンテンツと媒体鍵と装置鍵とを可搬媒体１４に書き込む。可搬媒体１４が携帯情報端末１５に挿入されると、携帯情報端末１５は、第２暗号化コンテンツを媒体鍵で復号し、再生する。

明 細 書

記録再生装置及びコンテンツ保護システム

技術分野

[0001] 本発明は、コンテンツを記録再生する記録再生装置に関し、特にコンテンツの不正利用を防止しつつユーザの利便性を高める技術に関する。

背景技術

[0002] デジタル放送番組のコピーガード施策として、1回だけ録画可能であることを示す「コピーワンス」の制御信号を付加して暗号化して放送される。この様に「コピーワンス」の制御信号が付加されたデジタル放送番組は、CPRM(Content Protection for Recordable Media)に対応する記録再生装置を用いることにより録画することができる。録画されたデジタル放送番組は、他の機器にダビングすることはできず、対応する機器への移動(ムーブ)のみ行うことができる。

特許文献1:特開2003-228522号公報

非特許文献1:「現代暗号理論」、池野信一、小山謙二、電子通信学会

非特許文献2:「現代暗号入門」、岡本栄司、共立出版株式会社

発明の開示

発明が解決しようとする課題

[0003] しかしながら、デジタル放送番組は、データ量の多い高画質コンテンツであるため、移動先がメモリカードなど記憶容量の小さい機器である場合には、記録再生装置は、高画質コンテンツを画像変換により圧縮し、データ量を減らした後にメモリカードに移動させる必要がある。

この場合、移動先のメモリカードから元の記録再生装置へ再度コンテンツを移動させた場合には、既に画像変換により元の高画質コンテンツは失われてしまっているので、記録再生装置は、もはや高画質コンテンツを利用することができないという問題がある。

[0004] そこで本発明は、上記の問題点に鑑みなされたものであって、画像変換を施したコンテンツを他の機器へ移動した場合であっても、移動先の機器から元の記録再生装

置へ再度コンテンツを移動させた場合に、画像変換前のコンテンツを利用することができる記録再生装置及びコンテンツ保護システムを提供することを目的とする。

課題を解決するための手段

[0005] 上記の目的を達成するために、本発明は、コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置であって、コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶している記憶手段と、前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、前記復号手段により復号されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換手段と、前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶手段から読み出し、前記可搬媒体に書き込む書込手段とを備えることを特徴とする。

[0006] また、上記の目的を達成するために、前記鍵消去手段は、前記書込手段が、前記装置鍵を前記可搬媒体に書き込んだ後に、前記記憶手段から前記装置鍵を消去し、前記書込手段は、前記鍵消去手段が前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させることを特徴とする。

発明の効果

[0007] 本発明は、コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置であって、コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶領域に記憶しており、前記装置鍵を用いて前記第1暗号化コンテンツを復号し、復号したコンテンツに非可逆変換を施し、変換コンテンツを生成し、生成した前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成し、前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶領域から読み出し、前記可搬媒体に書き込み、前記記憶領域から前記装置鍵を消去することを特徴とする。

[0008] この構成によると、前記端末装置は、前記第2暗号化コンテンツと前記媒体鍵とを前記可搬媒体に移動させると共に、前記装置鍵も前記可搬媒体に移動させるので、

前記第1暗号化コンテンツを、記憶領域に格納したままで、コンテンツの利用を無効化することができる。

また、記憶領域に第1暗号化コンテンツを記憶しているため、前記第2暗号化コンテンツを前記可搬媒体に移動させた後であっても、前記装置鍵を取得することにより画像変換前の前記コンテンツを復元することが可能である。

[0009] ここで、前記端末装置は、前記装置鍵を前記可搬媒体に書き込んだ後に、記憶領域から前記装置鍵を消去し、前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させるように構成してもよい。

この構成によると、第1暗号化コンテンツを復号するための装置鍵を消去した後に、第2暗号化コンテンツと第2暗号化コンテンツを復号するための媒体鍵とを可搬媒体に移動させるため、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0010] ここで、前記端末装置は、前記装置鍵を暗号化するための鍵情報を記憶しており、前記鍵情報を用いて前記装置鍵を暗号化し、暗号化装置鍵を生成し、前記装置鍵に替えて、生成された前記暗号化装置鍵を前記可搬媒体に書き込むように構成してもよい。

この構成によると、装置鍵を暗号化せず可搬媒体に書き込む場合と比較し、安全に装置鍵を可搬媒体に書き込むことができる。

[0011] ここで、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記暗号化装置鍵を前記可搬媒体に書き込み、前記装置鍵を消去した後の前記端末装置は、前記暗号化装置鍵を前記可搬媒体から読み出し、前記鍵情報を用いて前記暗号化装置鍵を復号し、前記装置鍵を生成し、生成した前記装置鍵を記憶領域に格納するように構成してもよい。

[0012] この構成によると、可搬媒体に移動させた装置鍵を可搬媒体から読み出すことにより、端末装置は、コンテンツ利用不可状態から利用可能状態となる。このとき、端末装置は、記憶している第1暗号化コンテンツを可搬媒体から読み出した装置鍵を用いて復号することにより、変換前のコンテンツを復号することができる。

また、読み出す装置鍵が暗号化されていることにより、暗号化されていない装置鍵

を読み出す場合と比較し、安全に装置鍵を可搬媒体から読み出すことができる。

[0013] ここで、前記端末装置は、更に、変換されて生成された前記変換コンテンツに、前記装置鍵を埋め込み、鍵埋込コンテンツを生成し、生成された前記鍵埋込コンテンツを、前記媒体鍵を用いて暗号化することにより前記第2暗号化コンテンツを生成し、前記装置鍵を前記変換コンテンツに埋め込んだ後に、記憶領域から前記装置鍵を消去し、前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させるように構成してもよい。

[0014] この構成によると、装置鍵を可搬媒体に書き込む場合と比較し、安全に装置鍵を可搬媒体に移動させることができる。また、装置鍵を消去した後に、第2暗号化コンテンツと第2暗号化コンテンツを復号するための媒体鍵とを可搬媒体に移動させるため、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0015] ここで、前記端末装置は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記記憶手段から前記装置鍵を消去した後に、前記可搬媒体から前記第2暗号化コンテンツ及び前記媒体鍵を読み出し、前記媒体鍵を用いて前記第2暗号化コンテンツを復号し、前記鍵埋込コンテンツを生成し、前記鍵埋込コンテンツから前記装置鍵を抽出し、抽出した前記装置鍵を前記記憶手段に格納するように構成してもよい。

[0016] この構成によると、端末装置は、可搬媒体に移動させた装置鍵を取得することにより、コンテンツ利用不可状態から利用可能状態となる。このとき、端末装置は、記憶している第1暗号化コンテンツを抽出した装置鍵を用いて復号することにより、変換前のコンテンツを復号することができる。

ここで、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記装置鍵を前記可搬媒体に書き込み、前記鍵消去手段は、前記記憶手段から、前記装置鍵を消去した後の前記端末装置は。前記可搬媒体から前記装置鍵を読み出し、読み出した前記装置鍵を、前記記憶手段に格納するように構成してもよい。

[0017] この構成によると、端末装置は、可搬媒体に移動させた装置鍵を取得することにより、コンテンツ利用不可状態から利用可能状態となる。このとき、端末装置は、記憶し

ている第1暗号化コンテンツを抽出した装置鍵を用いて復号することにより、変換前のコンテンツを復号することができる。

ここで、前記端末装置は、更に、記憶領域から前記第1暗号化コンテンツと前記装置鍵とを読み出し、読み出した前記装置鍵を用いて前記第1暗号化コンテンツを復号して前記コンテンツを生成し、生成した前記コンテンツを再生するように構成してもよい。

[0018] この構成によると、記憶領域に装置鍵が格納されており、コンテンツを利用可能状態である端末装置は、第1暗号化コンテンツを前記装置鍵を用いて復号し、再生することができる。

また、本発明は、コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置であって、コンテンツが暗号化されて生成された第1暗号化コンテンツとコンテンツ鍵とを記憶しており、前記コンテンツ鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成し、生成された前記コンテンツに非可逆変換を施し、変換コンテンツを生成し、生成された前記変換コンテンツを、前記コンテンツ鍵を用いて暗号化し、第2暗号化コンテンツを生成し、前記コンテンツ鍵及び前記第2暗号化コンテンツとを、前記可搬媒体に移動させ、記憶領域から前記コンテンツ鍵を消去することを特徴とする。

[0019] この構成によると、前記端末装置は、前記第2暗号化コンテンツと前記コンテンツ鍵とを前記可搬媒体に移動させると共に、記憶領域からコンテンツ鍵を消去することで、前記第1暗号化コンテンツを、記憶領域に格納したままで、コンテンツの利用を無効化することができる。

また、記憶領域に第1暗号化コンテンツを記憶しているため、前記第2暗号化コンテンツを前記可搬媒体に移動させた後であっても、前記コンテンツ鍵を取得すれば画像変換前の前記コンテンツを復元することが可能である。

[0020] ここで、前記端末装置は、前記コンテンツ鍵を前記可搬媒体に書き込んだ後に、記憶領域から前記コンテンツ鍵を消去し、前記コンテンツ鍵を消去した後に、前記第2暗号化コンテンツを前記可搬媒体に移動させるように構成してもよい。

この構成によると、コンテンツ移動処理の過程において、端末装置及び可搬媒体が

共に、暗号化コンテンツとコンテンツ鍵とを保持する状態が存在しない。即ち、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0021] ここで、前記コンテンツ鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、記憶領域から、前記コンテンツ鍵を消去した後の前記端末装置は、前記可搬媒体から前記コンテンツ鍵を読み出し、読み出した前記コンテンツ鍵を、記憶領域に格納するように構成してもよい。

この構成によると、端末装置は、可搬媒体に移動させた装置鍵を取得することにより、コンテンツ利用不可状態から利用可能状態となる。このとき、端末装置は、記憶している第1暗号化コンテンツを抽出した装置鍵を用いて復号することにより、変換前のコンテンツを復号することができる。

[0022] また、本発明は、コンテンツの著作権を保護しつつ、コンテンツの利用権を端末装置から可搬媒体へ移動させるコンテンツ保護システムであって、前記端末装置は、コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを第1記憶領域に記憶しており、前記装置鍵を用いて前記第1暗号化コンテンツを復号して前記コンテンツを生成し、生成されたコンテンツに非可逆変換を施し、変換コンテンツを生成し、生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成し、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、記憶領域から前記装置鍵を読み出し、前記可搬媒体に書き込み、前記第1記憶領域から前記装置鍵を消去し、前記可搬媒体は、前記端末装置から受け取る前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを記憶する第2記憶領域を備え、前記端末装置は、前記装置鍵を前2記憶領域に書き込んだ後に、第1記憶領域から前記装置鍵を消去し、前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させることを特徴とする。

[0023] この構成によると、前記端末装置は、前記第2暗号化コンテンツと前記媒体鍵とを前記可搬媒体に移動させると共に、前記装置鍵も前記可搬媒体に移動させるので、前記第1暗号化コンテンツを、第1記憶領域に格納したままで、コンテンツの利用を無効化することができる。

また、前記端末装置は、前記第1記憶領域に前記第1暗号化コンテンツを記憶しているため、前記第2暗号化コンテンツを前記可搬媒体に移動させた後であっても、前記装置鍵を取得することにより画像変換前のコンテンツを復元することが可能である。

[0024] ここで、前記端末装置は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記装置鍵を前記可搬媒体に書き込み、前記記憶手段から、前記装置鍵を消去した後の前記コンテンツ保護システムにおいて、前記端末装置は、前記可搬媒体から前記装置鍵を読み出し、読み出した前記装置鍵を、第1記憶領域に格納し、前記可搬媒体は、第2記憶領域に格納されている前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去し、前記端末装置は、前記可搬媒体が前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去した後、前記装置鍵を読み出すように構成してもよい。

[0025] この構成によると、可搬媒体は、第2暗号化コンテンツ及び媒体鍵の少なくとも一方を消去することにより、第2暗号化コンテンツを利用不可能状態とすることができる。また、端末装置は、可搬媒体が第2暗号化コンテンツを利用不可能状態となった後に、装置鍵を読み出すため、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0026] ここで、前記端末装置は第1記憶領域に、前記装置鍵を暗号化するための鍵情報を記憶しており、前記鍵情報を用いて前記装置鍵を暗号化して暗号化装置鍵を生成し、前記装置鍵に替えて生成された前記暗号化装置鍵を前記第2記憶領域に書き込み、前記暗号化装置鍵を書き込んだ後に、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記憶手段に移動させ、前記第2記憶領域は、前記装置鍵に替えて、前記暗号化装置鍵を記憶するように構成してもよい。

[0027] この構成によると、装置鍵を暗号化せず可搬媒体に書き込む場合と比較し、安全に装置鍵を可搬媒体に書き込むことができる。また、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

ここで、前記端末装置は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬

媒体に移動させ、前記暗号化装置鍵を前記可搬媒体に書き込み、前記第1記憶領域から前記装置鍵を消去した後の前記コンテンツ保護システムであって、前記端末装置は、前記暗号化装置鍵を前記第2記憶領域から読み出し、前記鍵情報を用いて前記暗号化装置鍵を復号して前記装置鍵を生成し、生成した前記装置鍵を前記第1記憶領域に格納し、前記可搬媒体は、前記第2記憶領域に格納されている前記第2暗号化コンテンツ及び前記媒体鍵の内、少なくとも一方を消去し、前記端末装置は前記可搬媒体が、前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去した後、前記暗号化装置鍵を読み出すように構成してもよい。

[0028] この構成によると、可搬媒体に移動させた暗号化装置鍵を可搬媒体から読み出し、復号することにより、端末装置は、コンテンツ利用不可状態から利用可能状態となる。このとき、端末装置は、記憶している第1暗号化コンテンツを可搬媒体から読み出した装置鍵を用いて復号することにより、変換前のコンテンツを復号することができる。

また、可搬媒体から読み出す装置鍵が暗号化されていることにより、暗号化されていない装置鍵を読み出す場合と比較し、安全に装置鍵を可搬媒体から読み出すことができる。また、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0029] ここで、前記端末装置は、前記変換コンテンツに、前記装置鍵を埋め込み、鍵埋込コンテンツを生成し、生成した前記鍵埋込コンテンツを、前記媒体鍵を用いて暗号化することにより前記第2暗号化コンテンツを生成し、前記鍵消去手段は、前記装置鍵を前記変換コンテンツに埋め込んだ後に、前記第1記憶手段から前記装置鍵を消去し、前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記憶手段に書き込むように構成してもよい。

[0030] この構成によると、装置鍵を可搬媒体に書き込む場合と比較し、安全に装置鍵を可搬媒体に移動させることができる。また、装置鍵を消去した後に、第2暗号化コンテンツと第2暗号化コンテンツを復号するための媒体鍵とを可搬媒体に移動させるため、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0031] ここで、前記端末装置は、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記

憶手段に移動させ、前記第1記憶領域から前記装置鍵を消去した後の前記コンテンツ保護システムであって、前記端末装置は、前記第2記憶領域から前記第2暗号化コンテンツ及び前記媒体鍵を読み出し、前記媒体鍵を用いて前記第2暗号化コンテンツを復号し、前記鍵埋込コンテンツを生成し、生成した前記鍵埋込コンテンツから前記装置鍵を抽出し、抽出した前記装置鍵を前記第1記憶領域に格納し、前記可搬媒体は、前記端末装置により、前記第2暗号化コンテンツ及び前記媒体鍵が読み出されると、前記第2記憶領域から、前記第2暗号化コンテンツ及び前記媒体鍵を消去するように構成してもよい。

[0032] この構成によると、端末装置は、可搬媒体に移動させた装置鍵を取得することにより、コンテンツ利用不可状態から利用可能状態となる。このとき、端末装置は、記憶している第1暗号化コンテンツを抽出した装置鍵を用いて復号することにより、変換前のコンテンツを復号することができる。また、可搬媒体は、第2暗号化コンテンツと媒体鍵とを消去することにより、端末装置及び可搬媒体が同時にコンテンツ利用可能状態となることはなく、ユーザは規格の範囲内でコンテンツを利用することができる。

[0033] ここで、前記コンテンツ保護システムは、更に、携帯情報端末を含み、前記携帯情報端末は、前記第2記憶領域に、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツが記憶された前記可搬媒体から、前記第2暗号化コンテンツと前記媒体鍵とを読み出し、読み出した前記第2暗号化コンテンツを、前記媒体鍵を用いて復号して、前記変換コンテンツを生成し、生成した前記変換コンテンツを再生するように構成してもよい。

[0034] この構成によると、ユーザは、可搬媒体が端末装置から取得した第2暗号化コンテンツを携帯情報端末を用いて再生することにより視聴することができる。

ここで、前記コンテンツ保護システムは、更に、前記端末装置と接続された他の端末装置を備え、前記他の端末装置は、前記第2記憶領域に、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツが記憶された前記可搬媒体から、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを読み出し、読み出した前記媒体鍵及び前記第2暗号化コンテンツの内少なくとも一方を消去し、前記媒体鍵及び前記第2暗号化コンテンツの内少なくとも一方が消去されると、前記端末装置から前記第1暗号化

コンテンツを取得し、前記可搬媒体は、前記他の端末装置へ前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを移動させ、前記端末装置は、更に、前記他の端末装置へ、前記第1暗号化コンテンツを送信し、前記第1記憶領域から前記第1暗号化コンテンツを消去するように構成してもよい。

[0035] この構成によると、端末装置、可搬媒体及び他の端末装置が同時にコンテンツ利用可能状態となることはなく、可搬媒体から他の端末装置へコンテンツを移動させることもでき、よりユーザの利便性が高まる。

図面の簡単な説明

[0036] [図1]コンテンツ保護システム1の構成を示す図である。

[図2]記録再生装置10の構成を機能的に示す機能ブロック図である。

[図3]記憶部104が記憶している情報を示す図である。

[図4]モニタ12に出力されるタイトルリストの具体例を示す図である。

[図5]可搬媒体14の構成を機能的に示す機能ブロック図である。

[図6]携帯電話機15の構成を機能的に示す機能ブロック図である。

[図7]コンテンツ保護システム1全体の動作を示すフローチャートである。

[図8]記録再生装置10から可搬媒体14へコンテンツをムーブする処理の動作を示すフローチャートである。

[図9]記録再生装置10から可搬媒体14へコンテンツをムーブする処理の過程において、記録再生装置10及び可搬媒体14が保持するデータを示す図である。

[図10]可搬媒体14から記録再生装置10へコンテンツをムーブする処理の動作を示すフローチャートである。

[図11]可搬媒体14から記録再生装置10へコンテンツをムーブする処理過程において、記録再生装置10及び可搬媒体14が保持するデータを示す図である。

[図12]コンテンツ保護システム1aの構成を示す図である。

[図13]PC16の構成を機能的に示す機能ブロック図である。

[図14]コンテンツ保護システム1a全体の動作を示すフローチャートである。

[図15]可搬媒体14からPC16へコンテンツをムーブする処理の動作を示すフローチャートであり、図16へ続く。

[図16]可搬媒体14からPC16へコンテンツをムーブする処理の動作を示すフローチャートであり、図15から続く。

[図17]コンテンツ保護システム2の構成及び記録再生装置20の機能的な構成を示す図である。

[図18]記録再生装置20から可搬媒体14へコンテンツをムーブする処理の動作を示すフローチャートである。

[図19]記録再生装置20から可搬媒体14へコンテンツをムーブする処理の過程において、記録再生装置10及び可搬媒体14が保持するデータを示す図である。

[図20]可搬媒体14から記録再生装置20へコンテンツをムーブする処理の動作を示すフローチャートである。

[図21]可搬媒体14から記録再生装置20へコンテンツをムーブする処理過程において、記録再生装置20及び可搬媒体14が保持するデータを示す図である。

[図22]コンテンツ保護システム3の構成及び記録再生装置30の機能的な構成を示す図である。

[図23]記録再生装置30から可搬媒体14へコンテンツをムーブする処理の動作を示すフローチャートである。

[図24]記録再生装置30から可搬媒体14へコンテンツをムーブする処理の過程において、記録再生装置30及び可搬媒体14が保持するデータを示す図である。

[図25]可搬媒体14から記録再生装置30へコンテンツをムーブする処理の動作を示すフローチャートである。

[図26]可搬媒体14から記録再生装置30へコンテンツをムーブする処理過程において、記録再生装置30及び可搬媒体14が保持するデータを示す図である。

[図27]本発明に係る著作権保護システムの全体構成を示すブロック図である。

[図28]本発明の実施の形態1における機能ブロック図である。

[図29]本発明の実施の形態1における記録再生装置にコンテンツを記録する際の動作フロー図である。

[図30]本発明の実施の形態1における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー図である。

[図31]本発明の実施の形態1における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図である。

[図32]本発明の実施の形態1における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図である。

[図33]本発明の実施の形態1における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー図である。

[図34]本発明の実施の形態1における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図である。

[図35]本発明の実施の形態1における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図である。

[図36]本発明の実施の形態1における記録再生装置に記録したコンテンツを再生する際の動作フロー図である。

[図37]本発明の実施の形態1における機能ブロック図である。

[図38]本発明の実施の形態2における記録再生装置にコンテンツを記録する際の動作フロー図である。

[図39]本発明の実施の形態2における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー図である。

[図40]本発明の実施の形態2における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図である。

[図41]本発明の実施の形態2における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図である。

[図42]本発明の実施の形態2における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー図である。

[図43]本発明の実施の形態2における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図である。

[図44]本発明の実施の形態2における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図である。

[図45]本発明の実施の形態2における記録再生装置に記録したコンテンツを再生す

る際の動作フロー図である。

符号の説明

[0037] 1 コンテンツ保護システム

1a コンテンツ保護システム

2 コンテンツ保護システム

3 コンテンツ保護システム

10 記録再生装置

11 コンテンツ供給装置

12 モニタ

13 スピーカ

14 可搬媒体

15 携帯情報端末

16 PC

20 記録再生装置

30 記録再生装置

101 コンテンツ受信部

102 装置記録鍵記憶部

103 暗号化部

104 記憶部

105 復号部

106 再生部

107 変換部

108 媒体記録鍵生成部

109 媒体記録鍵記憶部

110 暗号化部

111 装置固有鍵記憶部

112 暗号化／復号部

113 書込／読出部

114 入力部

115 記録制御部

132 入出力部

133 記録制御部

134 記憶部

141 入出力部

142 制御部

143 ディスプレイ

144 キー操作部

145 通信部

146 アンテナ

147 マイク

148 スピーカ

161 入出力部

162 入力部

163 コンテンツ記憶部

164 媒体記録鍵記憶部

165 復号部

166 送受信部

167 復号部

168 復号部

169 暗号化部

170 記憶部

171 装置記録鍵記憶部

172 復号部

173 再生部

174 ディスプレイ

175 スピーカ

2001　鍵埋込／抽出部

2002　暗号化／復号部

3001　コンテンツ鍵記憶部

3002　コンテンツ鍵領域

発明を実施するための最良の形態

[0038] ＜実施例1＞

本発明に係る第1の実施例として、コンテンツ保護システム1について、図面を参照して説明する。

＜構成＞

1. システム全体

図1は、コンテンツ保護システム1の構成を示す図である。同図に示す様に、コンテンツ保護システム1は、記録再生装置10、コンテンツ供給装置11、モニタ12、スピーカ13、可搬媒体14及び携帯情報端末15から構成される。

[0039] コンテンツ保護システム1は、放送局に設置されたコンテンツ供給装置11から放送されるデジタル放送番組であるコンテンツを、記録再生装置10により受信し、受信したコンテンツを記録及び再生し、また、記録再生装置10に記録されているコンテンツを可搬媒体14へムーブ（移動）し、可搬媒体14にムーブされたコンテンツを、携帯情報端末15により再生する。更に、可搬媒体14に記録されているコンテンツを再度記録再生装置10へムーブするシステムである。

[0040] 2. コンテンツ供給装置11

コンテンツ供給装置11は、放送局に備えられており、MPEG（Moving Picture Experts Group phase）-2規格に従って圧縮符号化されたトランスポートストリームであるコンテンツを放送する。コンテンツ供給装置11から放送されたコンテンツは、記録再生装置10のアンテナにより受信される。

[0041] 3. 記録再生装置10

図2は、記録再生装置10の構成を機能的に示す機能ブロック図である。

同図に示す様に、記録再生装置10は、コンテンツ受信部101、装置記録鍵記憶部102、暗号化部103、記憶部104、復号部105、再生部106、変換部107、媒体記

録鍵生成部108、媒体記録鍵記憶部109、暗号化部110、装置固有鍵記憶部111、暗号化／復号部112、書込／読出部113、入力部114及び記録制御部115から構成される。

[0042] 記録再生装置10は、マイクロプロセッサ、ROM、RAM、ハードディスクユニット等を備えるコンピュータシステムであって、ここでは具体例としてハードディスクレコーダを想定している。

(1)コンテンツ受信部101

コンテンツ受信部101は、アンテナを含み、コンテンツ供給装置11から放送されたコンテンツを、アンテナを介して受信し、受信したコンテンツを暗号化部103へ出力する。なお、コンテンツ受信部101が受信するコンテンツは、MPEG-2規格に従い圧縮符号化された高画質コンテンツである。

[0043] (2)装置記録鍵記憶部102

装置記録鍵記憶部102は、予め内部に装置記録鍵K_{HDD}を記憶している。装置記録鍵K_{HDD}は、コンテンツ受信部101がコンテンツ供給装置11から受信したコンテンツを暗号化部103が暗号化する際に、暗号鍵として用いる128ビットのデータである。

装置記録鍵記憶部102は、装置記録鍵K_{HDD}が暗号化／復号部112により読み出されると、それまで記憶していた装置記録鍵K_{HDD}を消去する。また、装置記録鍵記憶部102は、暗号化／復号部112により、装置記録鍵K_{HDD}が書き込まれると、書き込まれた装置記録鍵K_{HDD}を再度格納する。

[0044] (3)暗号化部103

暗号化部103は、コンテンツ受信部101からコンテンツを受け取る。ここで暗号化部103が受け取るコンテンツは、高画質なMPEG-2コンテンツであり、後に説明するMPEG-4コンテンツと区別するために、「C2」と表記する。暗号化部103は、C2の先頭から128ビット毎に分割し、部分コンテンツを生成する。ここでは、生成した部分コンテンツを、それぞれ、$C2^{(1)}$、$C2^{(2)}$、$C2^{(3)}$、・・・、$C2^{(M)}$と表記する。

[0045] 更に、暗号化部103は、装置記録鍵記憶部102から装置記録鍵K_{HDD}を読み出し、部分コンテンツ$C2^{(n)}$(n＝1、2、・・・、Mである。以下同じ)のそれぞれについて、装置記録鍵K_{HDD}を暗号鍵として用い、暗号化アルゴリズムE_1を施して暗号化部分コン

テンツ$EC2^{(n)}$を生成する。即ち、$EC2^{(n)}=E_1(C2^{(n)}, K_{HDD})$である。なお、暗号化部103が用いる暗号化アルゴリズムE_1の一例は、AES(Advanced Encryption Standard)である。

[0046] 暗号化部103は、生成した暗号化部分コンテンツ$EC2^{(1)}$、$EC2^{(2)}$、・・・、$EC2^{(M)}$を記憶部104に格納する。

(4)記憶部104

記憶部104は、具体的にはハードディスクユニットであって、図3に示すように、暗号化コンテンツ領域104a、コンテンツテーブル領域104b及び機器ID領域104cを含む。

[0047] 記憶部104は、暗号化部103から暗号化部分コンテンツ$EC2^{(n)}$を受け取ると、暗号化コンテンツ領域104aに蓄積して格納する。なお、暗号化部分コンテンツ$EC2^{(n)}$が蓄積されて成るデータを、暗号化コンテンツEC2と表記する。

図3に示すように、暗号化コンテンツ領域104aは、暗号化コンテンツ$EC2_1$、$EC2_2$、$EC2_3$、・・・を格納している。添え字の数値は、単に、複数の暗号化コンテンツを識別するための情報である。各暗号化コンテンツEC2には、各暗号化コンテンツを一意に識別するための情報であるコンテンツIDが割り振られており、暗号化コンテンツ領域104aは、暗号化コンテンツとコンテンツIDとを対応付けて記憶している。具体的には、$EC2_1$のコンテンツIDは「CID__X」、$EC2_2$のコンテンツIDは「CID__A」、$EC2_3$のコンテンツIDは「CID__Y」である。

[0048] コンテンツテーブル領域104bは、コンテンツテーブル120を記憶している。コンテンツテーブル120は、暗号化コンテンツ領域104aに記憶されている暗号化コンテンツ$EC2_1$、$EC2_2$、$EC2_3$、・・・に関する情報を管理するテーブルである。図3に示すように、コンテンツテーブル120は、コンテンツ情報121、122、123、・・・を含む。

[0049] 各コンテンツ情報は、コンテンツID欄、タイトル欄、録画時間欄、利用可否欄、及びMOVE先機器欄を有し、各欄には、以下に示すデータが記述されている。

コンテンツID欄には、暗号化コンテンツ領域104aに記憶されている暗号化コンテンツのコンテンツIDが記述されている。タイトル欄には、コンテンツのタイトルが記述されている。コンテンツタイトルは、例えばEPGから取得する。録画時間欄には、コンテ

ンツの録画時間が記述されている。利用可否欄には、0又は1が記述されており、「0」は、コンテンツが利用不可能状態であることを示し、「1」はコンテンツが利用可能状態であることを示す。MOVE先機器欄には、コンテンツがムーブされている場合には、ムーブ先の機器を識別する機器IDが記述され、コンテンツがムーブされていない場合は、何も記述されない。

[0050] コンテンツテーブル120は、暗号化コンテンツ領域104aに新たに暗号化コンテンツが記録される毎に、対応する新たなコンテンツ情報を記憶する。なお、コンテンツ情報は、後述する記録制御部115により作成される。

機器ID領域104cは、記録再生装置10を一意に識別する機器ID「ID__A」を記憶している。機器ID「ID__A」は、予め設定されているものとする。

[0051] (5)復号部105

復号部105は、入力部114からコンテンツの指定とコンテンツをムーブする指示とを受け、記憶部104の暗号化コンテンツ領域104aから、指定の暗号化コンテンツを読み出す。具体的には、入力部114からコンテンツIDを受け付け、受け付けたコンテンツIDと一致するコンテンツIDを有する暗号化コンテンツを暗号化コンテンツ領域104aから読み出す。ここでは、コンテンツID「CID__A」を有する暗号化コンテンツ$EC2_2$を読み出したとする。復号部105は、暗号化コンテンツ$EC2_2$の先頭から128ビット毎に分割し、暗号化部分コンテンツを生成する。生成した暗号化部分コンテンツを、それぞれ、$EC2_2^{(1)}$、$EC2_2^{(2)}$、$EC2_2^{(3)}$、・・・、$EC2_2^{(M)}$とする。

[0052] 更に、復号部105は、装置記録鍵記憶部102に格納されている装置記録鍵K_{HDD}を読み出し、暗号化部分コンテンツ$EC2_2^{(n)}$のそれぞれについて、装置記録鍵K_{HDD}を復号鍵として用い、復号アルゴリズムD_1を施して部分コンテンツ$C2_2^{(n)}$を生成する。即ち、$C2_2^{(n)}=D_1(EC2_2^{(n)}, K_{HDD})$である。なお、復号アルゴリズム$D_1$は、暗号化アルゴリズム$E_1$で暗号化された暗号文を平文に変換するためのアルゴリズムである。

[0053] 復号部105は、生成した部分コンテンツ$C2_2^{(1)}$、$C2_2^{(2)}$、$C2_2^{(3)}$、・・・、$C2_2^{(M)}$を変換部107へ出力する。

また、復号部105は、コンテンツの再生時に、再生部106から指示を受け、記憶部104から読み出した暗号化コンテンツEC2を、装置記録鍵K_{HDD}を用いて復号し、復

号したコンテンツを再生部106へ出力する。

[0054] (6)再生部106

再生部106は、入力部114からコンテンツの指定とコンテンツを再生する指示を受け付け、受け付け指示を復号部105へ出力する。

再生部106は、具体的にはMPEGデコーダなどを含み、復号部105により復号されたコンテンツC2を受け取り、受け取ったコンテンツC2をデコードし、映像信号と音声信号とを生成する。再生部106は、生成した映像信号をモニタ12へ出力し、生成した音声信号をスピーカ13へ出力する。

[0055] また、再生部106は、入力部114からの指示を受け、記録制御部115からタイトルリストを読み出し、読み出したタイトルリストをモニタ12へ出力する。タイトルリストは、コンテンツテーブル領域104bに格納されているコンテンツテーブル120に基づき生成されたGUI用データである。その生成については、後述する。

図4(a)及び(b)は、タイトルリストの具体例を示す図である。図4(a)に示すタイトルリスト125は、タイトル情報126、127、128を含み、各タイトル情報は、タイトル欄、記録時間欄及び利用可否欄を含む。タイトル情報126は、コンテンツ情報121に対応し、タイトル情報127は、コンテンツ情報122に対応し、タイトル情報128は、コンテンツ情報123に対応している。各タイトル情報の利用可否欄は、「○」及び「×」の何れかが記載されており、「○」は当該コンテンツが利用可能状態であることを示し、「×」は当該コンテンツが利用不可能状態であることを示す。図4(b)に示すタイトルリスト129は、タイトル情報130及び131を含み、各タイトル情報は、タイトル欄及び記録時間欄を含む。タイトル情報130は、コンテンツ情報121に対応し、タイトル情報131は、コンテンツ情報123に対応している。即ち、タイトルリスト129は、利用不可能状態であるコンテンツについての情報を含まない。

[0056] ここで、先の再生するコンテンツの指定及びムーブするコンテンツの指定は、モニタ12にタイトルリスト125又は126が表示されている状態において、入力部114が何れかのタイトル情報を選択することにより受け付けるように構成してもよい。

(7)変換部107

変換部107は、具体的には、MPEG-2のデータを、MPEG-4に変換するための

ダウンコンバータなどから構成され、復号部105により生成される部分コンテンツC2(n)を順次受け取り、受け取った部分コンテンツ$C2^{(n)}$を、MPEG-4に圧縮変換する。ここで、MPEG-4に変換された部分コンテンツを$C4^{(n)}$と表記する。

[0057] 具体例として、変換部107は、復号部105から$C2_2^{(1)}$、$C2_2^{(2)}$、$C2_2^{(3)}$、・・・、$C2_2^{(M)}$を受け取り、$C4_2^{(1)}$、$C4_2^{(2)}$、$C4_2^{(3)}$、・・・、$C4_2^{(M)}$を生成する。変換部107、生成した部分コンテンツ$C4_2^{(1)}$、$C4_2^{(2)}$、$C4_2^{(3)}$、・・・、$C4_2^{(M)}$を順次、暗号化部110へ出力する。

なお、MPEG-2からMPEG-4への変換は公知技術により実現可能であるため説明を省略する。

[0058] (8)媒体記録鍵生成部108

媒体記録鍵生成部108は、乱数生成器などから構成され、媒体記録鍵K_Tを生成する。媒体記録鍵K_Tは、暗号化部110による暗号化の際に、暗号鍵として用いられる128ビットのデータである。媒体記録鍵生成部108は、生成した媒体記録鍵K_Tを、媒体記録鍵記憶部109へ出力する。

[0059] (9)媒体記録鍵記憶部109

媒体記録鍵記憶部109は、媒体記録鍵生成部108から媒体記録鍵K_Tを受け取り、受け取ったK_Tを内部に格納する。書込／読出部113により媒体記録鍵K_Tが可搬媒体14に書き込まれると、媒体記録鍵記憶部109は、格納している媒体記録鍵K_Tを消去する

(10)暗号化部110

暗号化部110は、変換部107から、部分コンテンツを$C4^{(n)}$を順次受け取る。 更に、暗号化部110は、媒体記録鍵記憶部109から装置記録鍵K_Tを読み出し、部分コンテンツ$C4^{(n)}$のそれぞれについて、媒体記録鍵K_Tを暗号鍵として用い、暗号化アルゴリズムE_2を施して暗号化部分コンテンツ$EC4^{(n)}$を生成する。即ち、$EC4^{(n)}=E_2(C4^{(n)}, K_T)$である。なお、暗号化部110が用いる暗号化アルゴリズムE_2の一例は、AESである。

[0060] ここでは、具体例として暗号化部110は、部分コンテンツ$C4_2^{(1)}$、$C4_2^{(2)}$、$C4_2^{(3)}$、・・・、$C4_2^{(M)}$を順次暗号化して$EC4_2^{(1)}$、$EC4_2^{(2)}$、$EC4_2^{(3)}$、・・・、$EC4_2^{(M)}$を生成するものとする。暗号化部110は、生成した暗号化部分コンテンツ$EC4_2^{(1)}$、$EC4_2^{(2)}$、$EC4_2^{(3)}$、・

・・、$EC4_2^{(M)}$を書込／読出部113へ出力する。

[0061] (11)装置固有鍵記憶部111

装置固有鍵記憶部111は、装置固有鍵Kaを予め保持している。装置固有鍵Kaは、装置記録鍵K_{HDD}を暗号化及び復号するための56ビットのデータである。

(12)暗号化／復号部112

暗号化／復号部112は、装置記録鍵記憶部102に格納されている装置記録鍵K_{HDD}を読み出し、更に、装置固有鍵記憶部111に格納されている装置固有鍵Kaを読み出す。暗号化／復号部112は、装置記録鍵K_{HDD}に装置固有鍵Kaを暗号鍵として用い、暗号化アルゴリズムE_3を施して暗号化装置記録鍵EK_{HDD}を生成し、生成した暗号化装置記録鍵EK_{HDD}を、記憶部104の機器ID領域104cから読み出した、機器ID「ID__A」と共に、書込／読出部113へ出力する。ここで、暗号化アルゴリズムE_3の一例は、DESである。

[0062] また、暗号化／復号部112は、書込／読出部113から暗号化装置記録鍵EK_{HDD}と機器IDとを受け取ると、受け取った機器IDが、機器ID領域104cに格納されている記録再生装置10の機器ID「ID__A」と一致するか否か判断する。

書込／読出部113から受け取った機器IDが「ID__A」と一致する場合には、暗号化／復号部112は、装置固有鍵記憶部111から装置固有鍵Kaを読み出し、暗号化装置記録鍵EK_{HDD}に装置固有鍵Kaを復号鍵として用い、復号アルゴリズムD_3を施して、装置記録鍵K_{HDD}を生成する。暗号化／復号部112は、生成した装置記録鍵K_{HDD}を、装置記録鍵記憶部102へ書き込む。

[0063] 書込／読出部113から受け取った機器IDが「ID__A」と一致しない場合、暗号化／復号部112は、受け取った機器ID及び暗号化装置記録鍵EK_{HDD}を破棄する。

ここで、復号アルゴリズムD_3は、暗号化アルゴリズムE_3を用いて暗号化した暗号文を平文に変換するためのアルゴリズムである。

(13)書込／読出部113

書込／読出部113は、メモリカードスロットを備え、メモリカードスロットに可搬媒体14が挿入されている状態において、暗号化部110から受け取る暗号化部分コンテンツ$EC4^{(n)}$、暗号化／復号部112から受け取る暗号化装置記録鍵EK_{HDD}及び機器ID「

ID__A」並びに媒体記録鍵記憶部109から受け取る媒体記録鍵K_Tを、可搬媒体14に書き込む。なお、書込／読出部113は、暗号化部110から暗号化部分コンテンツ$EC4^{(n)}$を受け取る毎に、順次可搬媒体14に書き込む。具体例として、書込／読出部113は、暗号化部分コンテンツ$EC4_2^{(1)}$、$EC4_2^{(2)}$、$EC4_2^{(3)}$、・・・、$EC4_2^{(M)}$を、可搬媒体14に書き込む。

[0064] また、書込／読出部113は、可搬媒体14から、暗号化装置記録鍵EK_{HDD}を読み出し、読み出した暗号化装置記録鍵を暗号化／復号部112へ出力する。

(14)入力部114

入力部114は、ユーザからの入力により指示を受け付け、受け付けた指示を、復号部105や、再生部106へ出力する。具体例として入力部114は、リモコンとリモコン受光部とから構成されてもよい。入力部114が受け付ける指示は、再生指示、ムーブ指示、タイトルリスト表示指示などである。

[0065] 再生指示は、記憶部104に記憶されている暗号化コンテンツを復号してモニタ12及びスピーカ13に出力することを示す。ムーブ指示は、記憶部104に記憶されている暗号化コンテンツを圧縮変換し、可搬媒体14へムーブすることを示す。

(15)記録制御部115

記録制御部115は、暗号化コンテンツが記憶部104の暗号化コンテンツ領域104aに記録される都度、記録された暗号化コンテンツに対応するコンテンツ情報を作成し、作成したコンテンツ情報をコンテンツテーブル領域104bのコンテンツテーブル120に追加して書き込む。更に、記録制御部115は、可搬媒体14へムーブされたことにより、利用不可能状態となったコンテンツについて、コンテンツ情報の利用可否欄のデータを「1」から「0」に変更する。同様に、コンテンツが可搬媒体からムーブされたことにより、利用可能状態となったコンテンツについて、コンテンツ情報の利用可否欄のデータを「0」から「1」に変更する。

[0066] 更に、記録制御部115は、コンテンツテーブル120から、タイトルリストを生成する。記録制御部115が生成するタイトルリストの一例は、図4(a)に示したタイトルリスト125である。記録制御部115は、コンテンツテーブル120に含まれる全てのコンテンツ情報について、各コンテンツ情報毎に、タイトル欄及び記録時間欄に記述されている

情報を抽出し、利用可否欄に記述されている情報が「1」の場合は「○」を、「0」の場合は「×」を生成し、タイトル欄、記録時間欄及び利用可否欄から成るタイトル情報を作成する。記録制御部115は、全てのコンテンツ情報からタイトル情報を作成することによりタイトルリスト125を作成して内部に保持する。

[0067] なお、記録制御部115は、図4(b)に示したタイトルリスト129を作成してもよい。この場合、記録制御部115は、コンテンツテーブル120から、利用可否欄に「1」を含むコンテンツ情報を全て抽出し、抽出した全てのコンテンツ情報について、各コンテンツ情報毎に、タイトル欄及び記録時間欄に記述されている情報を抽出し、タイトル欄及び記録時間欄から成るタイトル情報を作成する。記録制御部115は、抽出した全てのコンテンツ情報からタイトル情報を作成することによりタイトルリスト129を作成して内部に保持する。

[0068] 4. モニタ12及びスピーカ13

モニタ12及びスピーカ13は、具体的には、記録再生装置10と接続されたデジタルテレビである。モニタ12は、再生部106から映像信号を受け取ると、受け取った映像信号を出力する。スピーカ13は、再生部106から音声信号を受け取ると、受け取った音声信号を出力する。

[0069] 5. 可搬媒体14

図5は、可搬媒体14の構成を機能的に示す機能ブロック図である。同図に示す様に、可搬媒体14は、入出力部132、記録制御部133及び記憶部134から構成され、記憶部134は、暗号化コンテンツ領域134a、媒体記録鍵領域134b、暗号化装置記録鍵領域134c及び機器ID領域134dを含む。

[0070] 可搬媒体14は、記録再生装置10及び携帯情報端末15のメモリカードスロットに挿入されて使用される、カード型メモリである。可搬媒体14の具体例は、SDメモリカードである。

可搬媒体14は、記録再生装置10のメモリカードスロットに挿入されている状態において、記録再生装置10から暗号化コンテンツをムーブされる。ムーブされた暗号化コンテンツは、暗号化コンテンツ領域134aに格納される。暗号化コンテンツ領域134aに格納された暗号化コンテンツは、可搬媒体14が、携帯情報端末15のメモリカード

スロットに挿入されている状態において、携帯情報端末15を用いて再生することができる。また、暗号化コンテンツ領域134aに格納された暗号化コンテンツは、可搬媒体14が記録再生装置10に装着されている状態において、再度、記録再生装置10にムーブすることができる。

(1)入出力部132

入出力部132は、コネクタピン、インターフェースドライバなどから成り、可搬媒体14が挿入されている装置との間でデータの入出力を行うインターフェースである。

[0071] 可搬媒体14が記録再生装置10のメモリカードスロットに挿入されている状態において、入出力部132は、記録再生装置10の書込／読出部113から、暗号化部分コンテンツ$EC4^{(n)}$、暗号化装置記録鍵EK_{HDD}、機器ID「ID__A」及び媒体記録鍵K_Tを受け取り、受け取った各データを、記録制御部133へ出力する。なお、入出力部132は、書込／読出部113から暗号化部分コンテンツ$EC4^{(n)}$を受け取る毎に、順次記録制御部133へ出力する。具体例として、入出力部132は、暗号化部分コンテンツ$EC4_2^{(1)}$、$EC4_2^{(2)}$、$EC4_2^{(3)}$、・・・、$EC4_2^{(M)}$を受け取る。また、入出力部132は、記録制御部133から暗号化装置記録鍵EK_{HDD}、機器ID「ID__A」及び機器ID「ID__B」を受け取ると、受け取った暗号化装置記録鍵EK_{HDD}、機器ID「ID__A」及び機器ID「ID__B」を、書込／読出部113へ出力する。

[0072] 可搬媒体14が携帯情報端末15のメモリカードスロットに挿入されている状態において、入出力部132は、記録制御部133から暗号化コンテンツEC4及び媒体記録鍵K_Tを受け取り、受け取った暗号化コンテンツEC4及び媒体記録鍵K_Tを、携帯情報端末15の入出力部141へ出力する。

(2)記録制御部133

(a)可搬媒体14が記録再生装置10に挿入されている状態

記録制御部133は、入出力部132から受け取る各データを、記憶部134のそれぞれの領域に書き込む。具体的には、記録制御部133は、入出力部132から受け取る暗号化部分コンテンツ$EC4^{(n)}$を、順次暗号化コンテンツ領域134aに書き込み、暗号化装置記録鍵EK_{HDD}及び機器ID「ID__A」を、暗号化装置記録鍵領域134cに書き込み、媒体記録鍵K_Tを、媒体記録鍵領域134bに書き込む。

[0073] また、コンテンツを記録再生装置10へムーブする際には、記録制御部133は、暗号化コンテンツ領域134aに格納されている暗号化コンテンツEC4及び媒体記録鍵領域134bに格納されている媒体記録鍵K_Tを消去する。暗号化コンテンツEC4及び媒体記録鍵K_Tが消去されると、記録制御部133は、暗号化装置記録鍵領域134cから、暗号化装置記録鍵EK_{HDD}を読み出し、読み出した暗号化装置記録鍵EK_{HDD}を、入出力部132へ出力する。

(b) 可搬媒体14が携帯情報端末15に挿入されている状態

記録制御部133は、暗号化コンテンツ領域134aに格納されている暗号化コンテンツEC4及び媒体記録鍵領域134bに格納されている媒体記録鍵K_Tを読み出し、読み出した暗号化コンテンツEC4及び媒体記録鍵K_Tを入出力部132へ出力する。

[0074] (3) 記憶部134

記憶部134は、具体的にはフラッシュメモリで構成される。

暗号化コンテンツ領域134aは、記録制御部133及び入出力部132を介して、記録再生装置10から受け取る暗号化部分コンテンツ$EC4^{(n)}$を蓄積して成る暗号化コンテンツEC4を記憶する。具体例として、暗号化コンテンツ領域134aは、暗号化部分コンテンツ$EC4_2^{(1)}$、$EC4_2^{(2)}$、$EC4_2^{(3)}$、・・・、$EC4_2^{(M)}$を受け取り、蓄積し、暗号化コンテンツ$EC4_2$を記憶する。

[0075] 媒体記録鍵領域134bは、記録制御部133及び入出力部132を介して、記録再生装置10から受け取る媒体記録鍵K_Tを記憶する。

暗号化装置記録鍵領域134cは、記録制御部133及び入出力部132を介して、記録再生装置10から受け取る暗号化装置記録鍵EK_{HDD}を記憶する。

機器ID領域134dは、可搬媒体14を一意に識別する機器ID「ID__B」を記憶している。機器ID「ID__B」は、予め設定されているものとする。

[0076] 8. 携帯情報端末15

図6は、携帯情報端末15の機能的な構成を示す機能ブロック図である。同図に示す様に、携帯情報端末15は、入出力部141、制御部142、ディスプレイ143、キー操作部144、通信部145、アンテナ146、マイク147及びスピーカ148から構成され、具体的には、無線電波を用いて通信を行う携帯電話器である。

[0077] また、携帯情報端末15は、CPU、ROM、RAM、メモリカードスロットなどを備えるコンピュータシステムである。

入出力部141は、メモリカードスロットなどから成り、メモリカードスロットに可搬媒体14が挿入されている状態において、可搬媒体14の暗号化コンテンツ領域134aに格納されている暗号化コンテンツEC4及び媒体記録鍵領域134bに格納されている媒体記録鍵K_T読み出し、読み出した暗号化コンテンツEC4及び媒体記録鍵K_Tを制御部142へ出力する。

[0078] 制御部142は、入出力部141から、暗号化コンテンツEC4及び媒体記録鍵K を受け取り、受け取った暗号化コンテンツEC4を先頭から128ビット毎の暗号化部分コンテンツ$EC4^{(n)}$に分割する。

制御部142は、暗号化部分コンテンツ$EC4^{(n)}$に媒体記録鍵K_Tを復号鍵として用い、復号アルゴリズムD_2を施して、順次部分コンテンツ$C4^{(n)}$を復号する。即ち、$C4^{(n)} = D_2(EC4^{(n)}, K_T)$である。なお、制御部142が用いる復号アルゴリズムD_2は、暗号化アルゴリズムE_2を用いて暗号化された暗号文を平文に変換するアルゴリズムである。

[0079] ここでは、具体例として制御部142は、暗号化部分コンテンツ$EC4_2^{(1)}$、$EC4_2^{(2)}$、$EC4_2^{(3)}$、・・・、$EC4_2^{(M)}$を順次復号して$C4_2^{(1)}$、$C4_2^{(2)}$、$C4_2^{(3)}$、・・・、$C4_2^{(M)}$を生成するものとする。

制御部142は、生成した部分コンテンツ$C4_2^{(n)}$を、順次デコードし、映像信号及び音声信号を生成する。制御部142は、生成した映像信号をディスプレイ143へ出力し、生成した音声信号をスピーカ148へ出力する。

[0080] キー操作部144、通信部145、アンテナ146、マイク147及びスピーカ148は、携帯電話器としての通常の通話、電子メール送受信などの機能を担う。これらの構成要素については、公知技術で実現可能であるため説明を省略する。

＜動作＞

ここでは、図7から図11に示すフローチャート等を用いて、コンテンツ保護システム1の処理動作について説明する。

[0081] 1．システム全体の動作

図7は、コンテンツ保護システム1全体の動作、及び各装置の状態を説明するフロ

ーチャートである。

コンテンツ供給装置11は、コンテンツを放送し(ステップS1)、記録再生装置10は、アンテナを介してコンテンツを受信する(ステップS2)。このとき、記録再生装置10は、コンテンツ利用可能状態である(ステップS3)。

[0082] コンテンツ利用可能状態である記録再生装置は、MPEG-2規格に従い圧縮符号化されたコンテンツが装置記録鍵K_{HDD}で暗号化された暗号化コンテンツEC2を記憶している。記録再生装置10は、暗号化コンテンツEC2を装置記録鍵K_{HDD}で復号し、コンテンツC2を生成し、生成したコンテンツC2をモニタ12及びスピーカ13に出力し、モニタ12及びスピーカ13は、コンテンツC2を再生する(ステップS11)。

[0083] コンテンツ利用可能状態(ステップS3)である記録再生装置10は、メモリカードスロットに挿入された可搬媒体14へコンテンツをムーブすることにより、コンテンツの利用権を可搬媒体14へ移動する(ステップS4)。コンテンツを可搬媒体14へムーブすると、記録再生装置10は、コンテンツ利用不可能状態となる(ステップS5)。

記録再生装置10からコンテンツをムーブされた可搬媒体14は、コンテンツ利用可能状態となる(ステップS6)。

[0084] コンテンツ利用可能状態である可搬媒体14は、MPEG-4規格に従い圧縮符号化されたコンテンツC4が媒体記録鍵K_Tで暗号化された暗号化コンテンツEC4、媒体記録鍵K_T及び暗号化装置記録鍵EK_{HDD}を記憶している。

可搬媒体14は、携帯情報端末15のメモリカードスロットに挿入され、暗号化コンテンツEC4及び媒体記録鍵K_Tを携帯情報端末15へ出力し、携帯情報端末15は、暗号化コンテンツEC4を媒体記録鍵K_Tで復号し、コンテンツC4を再生する(ステップS12)。

[0085] 続いて、可搬媒体14は、記録再生装置10のメモリカードスロットに挿入され、コンテンツを記録再生装置10へムーブすることにより、コンテンツの利用権を記録再生装置10へ移動する(ステップS7)。コンテンツを記録再生装置10へムーブすると、可搬媒体14は、コンテンツを利用不可能状態となる(ステップS8)。

可搬媒体14からコンテンツをムーブされた記録再生装置10は、コンテンツ利用可能状態となる(ステップS9)。コンテンツ利用可能状態である記録再生装置10は、コ

ンテンツC2をモニタ12及びスピーカ13に出力し、モニタ12及びスピーカ13は、コンテンツC2を再生する(ステップS11)。

[0086] 2. 記録再生装置10から可搬媒体14へのコンテンツ利用権移動処理の動作

図8は、記録再生装置10から可搬媒体14へのコンテンツのムーブ処理の動作を示すフローチャートである。ここに示す動作は、図7のステップS4の詳細である。

記録再生装置10の媒体記録鍵生成部108は、媒体記録鍵K_Tを生成し(ステップS101)。生成した媒体記録鍵K_Tを、媒体記録鍵記憶部109に格納する。

[0087] 次に、記録再生装置10は、記憶部104の暗号化コンテンツ領域104aに格納されている暗号化コンテンツEC2を、暗号化部分コンテンツ$EC2^{(n)}$に分割し、ステップS102からステップS112まで、n＝1，2，・・・，Mについて繰り返す。また、可搬媒体14は、ステップS107からステップS109まで、n＝1，2，・・・，Mについて繰り返す。

[0088] 先ず、記録再生装置10の復号部105は、暗号化部分コンテンツ$EC2^{(n)}$を、装置記録鍵K_{HDD}で復号し、部分コンテンツ$C2^{(n)}$を生成する(ステップS103)。次に、変換部107は、MPEG-2の部分コンテンツ$C2^{(n)}$をダウンコンして、MPEG-4の部分コンテンツ$C4^{(n)}$を生成する(ステップS104)。次に、暗号化部110は、部分コンテンツ$C4^{(n)}$を媒体記録鍵K_Tで暗号化し、暗号化部分コンテンツ$EC4^{(n)}$を生成する(ステップS105)。

[0089] 書込／読出部113は、暗号化部分コンテンツ$EC4^{(n)}$を、可搬媒体14に出力し、可搬媒体14の入出力部132は、暗号化部分コンテンツ$EC4^{(n)}$を受け取る(ステップS106)。可搬媒体14の記録制御部133は、入出力部141を介して暗号化部分コンテンツ$EC4^{(n)}$を受け取り、記憶部134の暗号化コンテンツ領域134aに書き込み、暗号化コンテンツ領域134aは、暗号化部分コンテンツ$EC4^{(n)}$を格納する(ステップS108)。暗号化コンテンツ領域134aにおいて、暗号化部分コンテンツ$EC4^{(n)}$が蓄積されることで、暗号化コンテンツEC4が生成される(ステップS110)。

[0090] 記録再生装置10は、ステップS106の出力が終了すると、暗号化部分コンテンツ$EC4^{(n)}$を消去する(ステップS111)。繰り返しが終了すると(ステップS112)、暗号化／復号部112は、装置記録鍵記憶部102から装置記録鍵K_{HDD}を読み出し、装置固有鍵記憶部111から装置固有鍵Kaを読み出す。暗号化／復号部112は、装置固有鍵

Kaを暗号鍵として用い、装置記録鍵K_{HDD}を暗号化し、暗号化装置記録鍵EK_{HDD}を生成する(ステップS113)。

[0091] 次に、暗号化／復号部112は、記憶部104の機器ID領域104cからID__Aを読み出し(ステップS114)、読み出したID__Aを、ステップS113で生成した暗号化装置記録鍵EK_{HDD}と共に、書込／読出部113へ出力する。書込／読出部113は、暗号化装置記録鍵EK_{HDD}とID__Aとを可搬媒体14へ出力し、可搬媒体14の入出力部132は、暗号化装置記録鍵EK_{HDD}とID__Aとを受け取る(ステップS115)。

[0092] 可搬媒体14の記録制御部133は、EK_{HDD}とID__Aとを、暗号化装置記録鍵領域134cに書き込み。暗号化装置記録鍵領域134cは、EK_{HDD}とID__Aとを格納する(ステップS116)。

記録再生装置10は、ステップS115の出力が終了すると、装置記録鍵記憶部102から、装置記録鍵K_{HDD}を消去する(ステップS117)。次に、書込／読出部113は、媒体記録鍵記憶部109から媒体記録鍵K_Tを読み出し(ステップS118)、読み出した媒体記録鍵K_Tを、可搬媒体14に出力し、可搬媒体14の入出力部132は、K_Tを受け取る(ステップS119)。

[0093] 可搬媒体14の記録制御部133は、媒体記録鍵K_Tを媒体記録鍵領域134bに書き込み、媒体記録鍵領域134bは、K_Tを格納する(ステップS120)。記録再生装置10は、ステップS119の出力が終了すると、媒体記録鍵記憶部109から、媒体記録鍵K_Tを消去する(ステップS121)。

可搬媒体14の記録制御部133は、媒体記録鍵K_Tを媒体記録鍵領域134bに書き込むと、機器ID領域134dからID__Bを読み出し(ステップS122)、入出力部132を介して、ID__Bを記録再生装置10へ出力し、記録再生装置10の書込／読出部113は、ID__Bを受け取る(ステップS123)。

[0094] 書込／読出部113は、受け取ったID__Bを記録制御部115へ出力する。記録制御部115は、ID__Bを受け取ると、記憶部104のコンテンツテーブル領域104b2格納されているコンテンツテーブル120から、ムーブしたコンテンツに対応するコンテンツ情報を特定し、特定したコンテンツ情報の、MOVE先機器欄に、ID__Bを書き込む(ステップS124)。

[0095] 図9は、記録再生装置10から可搬媒体14へ、コンテンツをムーブする処理の過程において、記録再生装置10及び可搬媒体14のそれぞれが保持するデータを説明する図面である。

(a)は、コンテンツをムーブする以前の記録再生装置10及び可搬媒体14が保持するデータを示している。

[0096] 記録再生装置10の暗号化コンテンツ領域104aは、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部109は、媒体記録鍵K_Tを記憶している。装置記録鍵記憶部102は、装置記録鍵K_{HDD}を記憶している。

可搬媒体14の暗号化コンテンツ領域134a、媒体記録鍵領域134b及び暗号化装置記録鍵領域134cは、何れもデータを保持していない。

[0097] このとき、記録再生装置10は、コンテンツ利用可能状態であり、MPEG-2コンテンツを利用できる。勿論、可搬媒体14は、コンテンツを保持しておらず、コンテンツ利用不可能状態である。

(b)は、暗号化コンテンツEC4の可搬媒体14への書き込みが終了した時点の記録再生装置10及び可搬媒体14が保持するデータを示している。

[0098] 記録再生装置10の暗号化コンテンツ領域104aは、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部109は、媒体記録鍵K_Tを記憶している。装置記録鍵記憶部102は、装置記録鍵K_{HDD}を記憶している。

可搬媒体14の暗号化コンテンツ領域134aは、MPEG-4の暗号化コンテンツEC4を記憶している。媒体記録鍵領域134b及び暗号化装置記録鍵領域134cは、何れもデータを保持していない。

[0099] このとき、記録再生装置10は、コンテンツ利用可能状態であり、MPEG-2コンテンツを利用できる。可搬媒体14は、暗号化されたMPEG-4コンテンツEC4を保持しているが、暗号化を解く媒体記録鍵K_Tを保持していないため、コンテンツ利用不可能状態である。

(c)は、装置記録鍵K_{HDD}の可搬媒体14への移動が終了した時点の記録再生装置10及び可搬媒体14が保持するデータを示している。

[0100] 記録再生装置10の暗号化コンテンツ領域104aは、MPEG-2の暗号化コンテンツ

EC2を記憶している。媒体記録鍵記憶部109は、媒体記録鍵K_Tを記憶している。装置記録鍵記憶部102は、データを保持していない。

可搬媒体14の暗号化コンテンツ領域134aは、MPEG-4の暗号化コンテンツEC4を記憶している。媒体記録鍵領域134bは、データを保持していない。暗号化装置記録鍵領域134cは暗号化装置記録鍵EK_{HDD}を記憶している。

[0101] このとき、記録再生装置10は、暗号化されたMPEG-2コンテンツを保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。可搬媒体14は、暗号化されたMPEG-4コンテンツを保持しているが、暗号化を解く媒体記録鍵K_Tを保持していないため、コンテンツ利用不可能状態である。

(d)は、コンテンツのムーブ処理が終了した時点の記録再生装置10及び可搬媒体14が保持するデータを示している。

[0102] 記録再生装置10の暗号化コンテンツ領域104aは、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部109及び装置記録鍵記憶部102は、何れもデータを保持していない。

可搬媒体14の暗号化コンテンツ領域134aは、MPEG-4の暗号化コンテンツEC4を記憶している。媒体記録鍵領域134bは、媒体記録鍵K_Tを記憶している。暗号化装置記録鍵領域134cは暗号化装置記録鍵EK_{HDD}を記憶している。

[0103] このとき、記録再生装置10は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。一方、可搬媒体14は、暗号化されたMPEG-4コンテンツEC4及び暗号化を解くための媒体記録鍵K_Tを保持しているため、コンテンツ利用可能状態である。

3. 可搬媒体14から記録再生装置10へのコンテンツ利用権移動処理の動作

図10は、可搬媒体14から記録再生装置10へのコンテンツのムーブ処理の動作を示すフローチャートである。ここに示す動作は、図7のステップS7の詳細である。

[0104] 可搬媒体14の記録制御部133は、記憶部134の媒体記録鍵領域134bから、媒体記録鍵K_Tを消去し(ステップS131)、更に、暗号化コンテンツ領域134aから、暗号化コンテンツEC4を消去する(ステップS132)。

次に、記録制御部133は、暗号化装置記録鍵領域134cから、暗号化装置記録鍵EK_{HDD}及び機器ID「ID__A」を読み出す(ステップS133)。読み出された暗号化装置記録鍵EK_{HDD}及びID__Aは、入出力部132を介して、記録再生装置10へ出力され、記録再生装置10の書込／読出部113は、暗号化装置記録鍵EK_{HDD}及びID__Aを受け取る(ステップS134)。書込／読出部113は、EK_{HDD}及びID__Aを暗号化／復号部112へ出力する。

[0105] 暗号化／復号部112は、受け取った機器ID「ID__A」が、自機の機器IDと一致するか否か確認する(ステップS135)。一致しない場合(ステップS136でNO)、書込／読出部113は、受け取った機器ID「ID__A」と暗号化装置記録鍵EK_{HDD}とを破棄する。その後、記録再生装置10は、エラーである旨をモニタ12に出力する等、エラー処理を行う(ステップS137)。

[0106] 受け取った機器ID「ID__A」が、自機の機器IDと一致する場合(ステップS136でYES)，暗号化／復号部112は、装置固有鍵記憶部111から装置固有鍵Kaを読み出し、装置固有鍵Kaを暗号鍵として用い、暗号化装置記録鍵EK_{HDD}を復号して、装置記録鍵K_{HDD}を生成する(ステップS138)。

暗号化／復号部112は、生成した装置記録鍵K_{HDD}を、装置記録鍵記憶部102に書き込み、装置記録鍵記憶部102は、K_{HDD}を格納する(ステップS139)。

[0107] 可搬媒体14の記録制御部133は、K_{HDD}が装置記録鍵記憶部102に格納されると、暗号化装置記録鍵領域134cに格納されている暗号化装置記録鍵EK_{HDD}及び機器ID「ID__A」を消去する(ステップS140)。

図11は、可搬媒体14から記録再生装置10へ、コンテンツをムーブする処理の過程において、記録再生装置10及び可搬媒体14のそれぞれが保持するデータを説明する図面である。

[0108] (a)は、コンテンツをムーブする以前の記録再生装置10及び可搬媒体14が保持するデータを示しており、図9(d)に示した状態と同一である。即ち、記録再生装置10は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。一方、可搬媒体14は、暗号化されたMPEG-4コンテンツEC4及び暗号化を解くための媒体記録

鍵K_Tを保持しているため、コンテンツ利用可能状態である。

[0109] (b)は、暗号化コンテンツEC4及び媒体記録鍵K_Tの消去が終了した時点の記録再生装置10及び可搬媒体14が保持するデータを示している。

記録再生装置10の暗号化コンテンツ領域104aは、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部109及び装置記録鍵記憶部102は、何れもデータを保持していない。

[0110] 可搬媒体14の暗号化コンテンツ領域134a及び媒体記録鍵領域134bは、何れもデータを保持していない。暗号化装置記録鍵領域134cは、暗号化装置記録鍵EK_{HDD}を保持している。

このとき、記録再生装置10は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。可搬媒体14は、コンテンツを保持しておらず、コンテンツを利用不可能状態である。

[0111] (c)は、コンテンツのムーブが終了した時点の記録再生装置10及び可搬媒体14が保持するデータを示している。

記録再生装置10の暗号化コンテンツ領域104aは、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部109は、データを保持していない。装置記録鍵記憶部102は、装置記録鍵K_{HDD}を記憶している。

[0112] 可搬媒体14の暗号化コンテンツ領域134a、媒体記録鍵領域134b及び暗号化装置記録鍵領域134cは、何れもデータを保持していない。

このとき、記録再生装置10は、コンテンツ利用可能状態であり、高画質なMPEG-2コンテンツを利用できる。可搬媒体14は、勿論、コンテンツ利用不可能状態である。

なお、本実施例では、可搬媒体14から記録再生装置10へコンテンツをムーブする際に、図10のステップS131において、まず可搬媒体14から媒体記録鍵K_Tを消去する構成としたが、この構成に限定されるものではない。

[0113] 例えば、ムーブ処理を行う際に、記録再生装置10は、可搬媒体14から、暗号化装置記録鍵領域134cに格納されている機器IDを読み出し、読み出した機器IDが、自

機の機器IDと一致するか否かを確認することにより、ムーブ対象となるコンテンツが、記録再生装置10自身が可搬媒体14にムーブしたコンテンツであるか否かを判定してもよい。

[0114] 機器IDが一致し、ムーブ対象となるコンテンツが、自機が可搬媒体14へムーブしたコンテンツであると判定する場合には、記録再生装置10は、その旨を可搬媒体14に通知し、通知を受けた可搬媒体14は、ステップS131から続けて動作するように構成してもよい。

機器IDが一致せず、ムーブ対象となるコンテンツが、自機が可搬媒体14へムーブしたコンテンツでないと判定する場合には、記録再生装置10は、その旨を可搬媒体14に通知し、通知を受けた可搬媒体14は、ムーブ処理を中止するように構成してもよい。

[0115] 或いは、ステップS131において、媒体記録鍵K_Tを消去せずに、媒体記録鍵K_Tの特定のビットを反転させたり、媒体記録鍵K_Tを一時待避用フォルダに移動したりするなどして一時的に無効化してもよい。この場合、ステップS136でYESの場合には、ステップS140の処理と共に一時的に無効化した媒体記録鍵K_Tを消去し、ステップS136でNOの場合には、ステップS137のエラー処理として、一時的に無効化した媒体記録鍵K_Tを有効化するように構成してもよい。

[0116] ＜変形例＞

ここでは、実施例1の変形例として、コンテンツ保護システム1aについて説明する。

図12は、コンテンツ保護システム1aのシステム構成を示す図である。同図に示す様に、コンテンツ保護システム1aは、記録再生装置10、コンテンツ供給装置11、モニタ12、スピーカ13、可搬媒体14、携帯情報端末15及びPC16から構成される。

[0117] コンテンツ保護システム1aは、コンテンツ保護システム1にPC16が追加された構成を有し、記録再生装置10とPC16とは、ケーブルを介して接続されている。

コンテンツ保護システム1aは、記録再生装置10から可搬媒体14にムーブされたコンテンツを、可搬媒体14からPC16へ更にムーブさせるシステムである。

コンテンツ供給装置11、モニタ12、スピーカ13、可搬媒体14及び携帯情報端末15は、コンテンツ保護システム1の構成要素と同一の機器であるため、ここでは説明を

省略する。

[0118] 1．記録再生装置10の構成

記録再生装置10は、先に述べた様にPC16と接続されており、図2に示した機能ブロック図の各構成要素に加えて、PC16とデータの送受信などを行う送受信部を備えるものとする。記録再生装置10の送受信部は、記憶部104及び装置固有鍵記憶部111に格納されているデータを読み出し、読み出したデータをPC16へ送信する。また、記録再生装置10の送受信部は、PC16から受け取る機器IDの確認処理を行う。

[0119] 2．PC16の構成

図13は、PC16の構成を機能的に示す機能ブロック図である。同図に示す様に、PC16は、入出力部161、入力部162、コンテンツ記憶部163、媒体記録鍵記憶部164、復号部165、送受信部166、復号部167、復号部168、暗号化部169、記憶部170、装置記録鍵記憶部171、復号部172、再生部173、ディスプレイ174及びスピーカ175から構成される。

[0120] PC16は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイ、キーボード、マウスなどを備えるコンピュータシステムである。なお、PC16と記録再生装置10とは、ケーブルで接続されているものとする。

(1)入出力部161

入出力部161は、メモリカードスロット、インターフェースドライバなどを含むメモリカードインターフェースであって、メモリカードスロットに可搬媒体14が挿入された状態において、可搬媒体14からデータを読み出す。

[0121] 具体的には、入出力部161は、入力部162からコンテンツの読み出しを示す信号を受け取ると、可搬媒体14の暗号化コンテンツ領域134aから、MPEG-4規格に従い圧縮符号化された暗号化コンテンツEC4を読み出し、読み出したEC4を、コンテンツ記憶部163へ書き込む。また、入出力部161は、可搬媒体の媒体記録鍵領域134bから媒体記録鍵K_Tを読み出し、読み出した媒体記録鍵K_Tを、媒体記録鍵記憶部164へ書き込む。また、入出力部161は、可搬媒体14の暗号化装置記録鍵領域134cから暗号化装置記録鍵EK_{HDD}を読み出し、読み出した暗号化装置記録鍵EK_{HDD}を、復号部167へ出力する。

[0122] (2)入力部162

入力部162は、キーボード及びマウスなどから構成され、キーボード及びマウスがユーザにより操作されることにより要求を受け付ける。入力部162は、受け付けた要求に対応する信号を生成し、生成した信号を、入出力部161、復号部165又は再生部173へ出力する。

[0123] (3)コンテンツ記憶部163

コンテンツ記憶部163は、入出力部161を介して、可搬媒体14から読み出したMPEG-4の暗号化コンテンツEC4を格納する。

(4)媒体記録鍵記憶部164

媒体記録鍵記憶部164は、入出力部161を介して、可搬媒体14から読み出した媒体記録鍵K_Tを格納する。

[0124] (5)復号部165

復号部165は、入力部162からMPEG-4コンテンツの再生を示す信号を受け取ると、コンテンツ記憶部163から暗号化コンテンツEC4を読み出し、媒体記録鍵記憶部164から、媒体記録鍵K_Tを読み出す。

復号部165は、暗号化コンテンツEC4を先頭から128ビット毎に分割し、それぞれを、暗号化部分コンテンツ$EC4^{(n)}$とする。

[0125] 復号部165は、K_Tを復号鍵として用い、暗号化部分コンテンツ$EC4^{(n)}$に復号アルゴリズムD_2を施すことにより部分コンテンツ$C4^{(n)}$を復号する。復号部165は、復号した$C4^{(n)}$を、順次再生部173へ出力する。

(6)送受信部166

送受信部166は、ケーブルコネクタなどを含み、ケーブルを介して接続された記録再生装置10から、MPEG-2規格に従い圧縮符号化された暗号化コンテンツEC2及び装置固有鍵Kaを受信する。送受信部166は、受信した暗号化コンテンツEC2を、復号部168へ出力し、受信した装置固有鍵Kaを、復号部167へ出力する。

[0126] (7)復号部167

復号部167は、入出力部161を介して可搬媒体14から読み出した暗号化装置記録鍵EK_{HDD}を受け取り、更に、送受信部166を介して記録再生装置10から装置固有

鍵Kaを受信する。

復号部167は、装置固有鍵Kaを復号鍵として用い、暗号化装置記録鍵EK_{HDD}に復号アルゴリズムD_3を施して、装置記録鍵K_{HDD}を復号する。復号部167は、復号した装置記録鍵K_{HDD}を、復号部168へ出力する。ここで、復号アルゴリズムD_3は、暗号化アルゴリズムE_3を用いて暗号化した暗号文を平文に変換するためのアルゴリズムである。

[0127] (8)復号部168

復号部168は、送受信部166を介して記録再生装置10から暗号化コンテンツEC2を受け取り、また、復号部167から装置記録鍵K_{HDD}を受け取る。

復号部168は、暗号化コンテンツEC2を、先頭から128ビット毎の暗号化部分コンテンツ$EC2^{(n)}$に分割する。復号部168は、暗号化部分コンテンツ$EC2^{(n)}$に装置記録鍵K_{HDD}を復号鍵として用い、復号アルゴリズムD_1を用いて復号し、部分コンテンツ$C2^{(n)}$を生成する。復号部168は、生成した部分コンテンツ$C2^{(n)}$を、順次暗号化部169へ出力する。

[0128] (9)暗号化部169

暗号化部169は、復号部168から部分コンテンツ$C2^{(n)}$を受け取る。

更に、暗号化部103は、装置記録鍵記憶部171から装置記録鍵K_{PC}を読み出し、部分コンテンツ$C2^{(n)}$のそれぞれについて、装置記録鍵K_{PC}を暗号鍵として用い、暗号化アルゴリズムE_1を施して暗号化部分コンテンツ$EC2^{(n)}$を生成する。即ち、$EC2^{(n)} = E_1(C2^{(n)}, K_{PC})$である。

[0129] 暗号化部169は、生成した暗号化部分コンテンツ$EC2^{(n)}$を記憶部170に格納する。

(10)記憶部170

記憶部170は、暗号化部169から出力される暗号化部分コンテンツ$EC2^{(n)}$を蓄積して成る暗号化コンテンツEC2を格納する。

[0130] (11)装置記録鍵記憶部171

装置記録鍵記憶部171は、予め内部に装置記録鍵K_{PC}を記憶している。装置記録鍵K_{PC}は、暗号化部169において暗号鍵として用いられ、且つ、復号部172において

復号鍵として用いられる128ビットのデータである。

(12)復号部172

復号部172は、記憶部170から、暗号化コンテンツEC2を読み出し、読み出した暗号化コンテンツEC2の先頭から128ビット毎に分割し、暗号化部分コンテンツ$EC2^{(n)}$を生成する。

[0131] 更に、復号部172は、装置記録鍵記憶部171に格納されている装置記録鍵K_{PC}を読み出し、暗号化部分コンテンツ$EC2^{(n)}$のそれぞれについて、装置記録鍵K_{PC}を復号鍵として用い、復号アルゴリズムD を施して部分コンテンツ$C2^{(n)}$を生成する。即ち、$C2^{(n)}=D_1(EC2^{(n)}, K_{PC})$である。なお、復号アルゴリズム$D_1$は、暗号化アルゴリズム$E_1$で暗号化された暗号文を平文に変換するためのアルゴリズムである。

[0132] 復号部172は、生成した部分コンテンツ$C2^{(n)}$を、順次再生部173へ出力する。

(13)再生部173

再生部173は、MPEG-2デコーダ及びMPEG-4デコーダを備える。

再生部173は、復号部165からMPEG-4規格に従い圧縮符号化されたコンテンツC4を受け取ると、受け取ったコンテンツC4をMPEG-4デコーダにてデコードし、映像信号と音声信号とを生成する。

[0133] 再生部173は、復号部172からMPEG-2規格に従い圧縮符号化されたコンテンツC2を受け取ると、受け取ったコンテンツC2をMPEG-2デコーダにてデコードし、映像信号と音声信号とを生成する。

再生部173は、生成した映像信号をディスプレイ174へ出力し、音声信号をスピーカ175へ出力する。

[0134] (14)ディスプレイ174及びスピーカ175

ディスプレイ174は、再生部173から映像信号を受け取り、映像信号を出力する。スピーカ175は、再生部173から音声信号を受け取り、音声信号を出力する。

3. システム全体の動作の動作

コンテンツ保護システム1a全体の動作及び各機器の状態について、図7及び図14に示すフローチャートを用いて説明する。

[0135] 先ず、図7に示したステップS1からステップS6について、コンテンツ保護システム1

aは、コンテンツ保護システム1と同様に動作する。ステップS6の続きから、図14へ続く。

コンテンツ利用不可能状態（ステップS5）である記録再生装置10、コンテンツ利用可能状態（ステップS6）である可搬媒体14、及びPC16との間で、コンテンツ利用権移動処理を行う（ステップS13）。

[0136] 記録再生装置10は、引き続きコンテンツ利用不可能状態であり（ステップS14）、コンテンツをムーブすることにより、可搬媒体14もコンテンツ利用不可能状態となる（ステップS15）。PC16は、コンテンツをムーブされコンテンツを利用可能状態である（ステップS16）。

コンテンツ利用可能状態である記録再生装置10は、コンテンツを出力し、再生する（ステップS17）。

[0137] 4. コンテンツ利用権移動処理の動作

ここでは、図15及び図16に示すフローチャートを用いて、可搬媒体14からPC16へコンテンツ利用権を移動させる処理の動作について説明する。なお、ここで説明する動作は、図14に示したフローチャートにおけるステップS13の詳細である。

メモリカードスロットに可搬媒体14が挿入されている状態において、PC16の入出力部161は、入力部162がユーザに操作されることにより、ムーブ要求を受け付ける（ステップS151）。ムーブ要求を受け付けると、入出力部161は、可搬媒体14へコンテンツの読み出し指示を出力する（ステップS152）。

[0138] 可搬媒体14の記録制御部133は、入出力部132を介して、コンテンツの読み出し指示を受け取ると、暗号化コンテンツ領域134aから、暗号化コンテンツEC4を読み出し（ステップS153）、入出力部132を介してPC16へ出力し、PC16の入出力部161は、暗号化コンテンツEC4を受け取る（ステップS154）。入出力部161は、受け取った暗号化コンテンツEC4を、コンテンツ記憶部163へ書き込み、コンテンツ記憶部163は、暗号化コンテンツEC4を格納する（ステップS155）。

[0139] 記録制御部133は、ステップS154におけるPC16への暗号化コンテンツEC4の出力が終了すると、暗号化コンテンツ領域134aから、暗号化コンテンツEC4を消去する（ステップS156）。

次に、記録制御部133は、媒体記録鍵領域134bから、媒体記録鍵K_Tを読み出し(ステップS157)、入出力部132を介してPC16へ出力し、PC16の入出力部161は、媒体記録鍵K_Tを受け取る(ステップS158)。入出力部161は、受け取った媒体記録鍵K_Tを、媒体記録鍵記憶部164へ書き込み、媒体記録鍵記憶部164は、媒体記録鍵K_Tを格納する(ステップS159)。可搬媒体14の記録制御部133は、媒体記録鍵領域134bから、媒体記録鍵K_Tを消去する(ステップS160)。

[0140] 記録制御部133は、ステップS158におけるPC16への媒体記録鍵K_Tの出力が終了すると、暗号化装置記録鍵領域134cから、暗号化装置記録鍵EK_{HDD}及びID__Aを読み出し(ステップS161)、読み出した暗号化装置記録鍵EK_{HDD}及びID__Aを、入出力部132を介してPC16へ出力し、PC16の入出力部161は、暗号化装置記録鍵EK_{HDD}及びID__Aを受け取る(ステップS162)。入出力部161は、受け取った暗号化装置記録鍵EK_{HDD}を、復号部167へ出力し、復号部167は、暗号化装置記録鍵EK_{HDD}を受け取り、内部に格納する(ステップS163)。また、入出力部161は、ID__Aを、送受信部166へ出力する。

[0141] 一方、可搬媒体14の記録制御部133は、暗号化装置記録鍵領域134cから、暗号化装置記録鍵EK_{HDD}及びID__Aを消去する(ステップS164)。

なお、ステップS159からステップS163までの間、PC16は、MPEG-4コンテンツを利用することができる。

PC16は、コンテンツ記憶部163に格納されている暗号化コンテンツEC4及び媒体記録鍵記憶部164に格納されている媒体記録鍵K_Tを消去する(ステップS165)。PC16は、暗号化コンテンツEC4及び媒体記録鍵K_Tの消去を確認後、送受信部166を介して、記録再生装置10へ、MPEG-2コンテンツを要求する(ステップS166)。

[0142] 具体的に、送受信部166は、MPEG-2コンテンツを要求する旨を示す信号と、入出力部161から受け取った機器ID「ID__A」とを、記録再生装置10へ送信し、記録再生装置10に備えられた送受信部は、MPEG-2コンテンツを要求する旨を示す信号と、機器ID「ID__A」とを受信する(ステップS167)。

記録再生装置10の送受信部は、記憶部104の機器ID領域104cから機器IDを読み出し、読み出した機器IDと受信した機器ID「ID__A」とが一致するか否か判断する

（ステップS168）。機器IDが一致しない場合（ステップS169でNO）、送受信部は、受信した機器ID「ID__A」を破棄し、PC16に対してエラーである旨を通知する（ステップS170）。

[0143] 機器IDが一致する場合（ステップS169でYES）、送受信部は、記憶部104の暗号化コンテンツ領域104aから、暗号化コンテンツEC2を読み出し、更に、装置固有鍵記憶部111から、装置固有鍵Kaを読み出す（ステップS171）。送受信部は、読み出した暗号化コンテンツEC2及び装置固有鍵KaをPC16へ送信し、PC16の送受信部166は、暗号化コンテンツEC4及び装置固有鍵Kaを受信する（ステップS172）。その後、記録再生装置10は、暗号化コンテンツEC2及び装置固有鍵Kaを消去する（ステップS173）。

[0144] PC16の送受信部166は、受信した装置固有鍵Kaを復号部167へ出力し、復号部167は、装置固有鍵Kaを用いてEK_{HDD}を復号し、装置記録鍵K_{HDD}を生成する（ステップS181）。復号部167は、生成した装置記録鍵K_{HDD}を、復号部168へ出力する。

また、送受信部166は、受信した暗号化コンテンツEC2を復号部168へ出力し、復号部168は、受け取った暗号化コンテンツEC2を、先頭から128ビット毎の暗号化部分コンテンツ$EC2^{(n)}$に分割する。

[0145] 次に、ステップS182からステップS186まで、n＝1，2，・・・，Mについて繰り返す。

復号部168は、暗号化部分コンテンツ$EC2^{(n)}$を装置記録鍵K_{HDD}を用いて復号し、部分コンテンツ$C2^{(n)}$を生成し（ステップS183）、生成した部分コンテンツ$C2^{(n)}$を、暗号化部169へ出力する。暗号化部169は、装置記録鍵記憶部171から装置記録鍵K_{PC}を読み出し、読み出した装置記録鍵K_{PC}を暗号鍵として用い、部分コンテンツ$C2^{(n)}$を暗号化して、暗号化部分コンテンツ$EC2^{(n)}$を生成する（ステップS184）。

[0146] 暗号化部169は、生成した暗号化部分コンテンツ$EC2^{(n)}$を、記憶部170へ格納する（ステップS185）。

＜実施例2＞

本発明における第2の実施例として、コンテンツ保護システム2について説明する。

＜構成＞

1．システム全体

図17は、コンテンツ保護システム2の構成、更には、記録再生装置20の機能的な構成を示す図である。同図に示す様に、コンテンツ保護システム2は、記録再生装置20、コンテンツ供給装置11．モニタ12、スピーカ13、可搬媒体14及び携帯情報端末15から構成される。

[0147] コンテンツ保護システム2は、コンテンツ保護システム1と同様に、放送局に設置されたコンテンツ供給装置11から放送されるデジタル放送番組であるコンテンツを、記録再生装置20が受信し、受信したコンテンツを記録及び再生し、また、記録再生装置20に記録されているコンテンツを可搬媒体14へムーブ（移動）し、ムーブされたコンテンツを、携帯情報端末15により再生する。更に、可搬媒体14に記録されているコンテンツを再度記録再生装置20へムーブするシステムである。

[0148] コンテンツ供給装置11及び携帯情報端末15は、それぞれ、コンテンツ保護システム1における装置と同一の機能及び構成を有する。

なお、図14に示した可搬媒体14は、入出力部132、記録制御部133及び機器ID領域134dを省略している。コンテンツ保護システム2における可搬媒体14は、暗号化装置記録鍵領域134cを備えていない。

[0149] 以下では、特に、コンテンツ保護システム1との相違点である記録再生装置20について説明する。

2．記録再生装置20

図17に示す様に、記録再生装置20は、コンテンツ受信部201、装置記録鍵記憶部202、暗号化部203、記憶部204、復号部205、再生部206、変換部207、媒体記録鍵生成部208、媒体記録鍵記憶部209、書込／読出部213、入力部214、記録制御部215、鍵埋込／抽出部2001及び暗号化／復号部2002から構成される。

[0150] 図2に示した記録再生装置10の機能ブロック図との相違は、記録再生装置20は、装置固有鍵記憶部111及び暗号化／復号部112に相当する構成要素を備えず、鍵埋込／抽出部2001及び暗号化／復号部2002を備える点である。

コンテンツ受信部201、装置記録鍵記憶部202、暗号化部203、記憶部204、復号部205、再生部206、変換部207、媒体記録鍵生成部208、媒体記録鍵記憶部2

09、書込／読出部213、入力部214及び記録制御部215は、図2に示したコンテンツ受信部101、装置記録鍵記憶部102、暗号化部103、記憶部104、復号部105、再生部106、変換部107、媒体記録鍵生成部108、媒体記録鍵記憶部109、書込／読出部113、入力部114及び記録制御部115と同様の構成及び機能を有するため、ここでは説明を省略する。

[0151] (1)鍵埋込／抽出部2001

鍵埋込／抽出部2001は、変換部207によりMPEG-2からMPEG-4に圧縮変換された部分コンテンツ$C4^{(n)}$を順次受け取り、蓄積する。更に、鍵埋込／抽出部2001は、装置記録鍵記憶部202から装置記録鍵K_{HDD}を読み出す。

鍵埋込／抽出部2001は、部分コンテンツ$C4^{(n)}$を蓄積して成るコンテンツC4に、装置記録鍵K_{HDD}を埋め込む。具体的には、鍵埋込／抽出部2001は、装置記録鍵K_{HDD}を、コンテンツC4のヘッダ部分にあるリザーブ領域に埋め込む。

[0152] 鍵埋込／抽出部2001は、装置記録鍵K_{HDD}を埋め込んだコンテンツC4を、暗号化／復号部2002へ出力する。

また、鍵埋込／抽出部2001は、暗号化／復号部2002から、装置記録鍵K_{HDD}が埋め込まれたコンテンツC4が128ビット毎に分割された部分コンテンツ$C4^{(n)}$を受け取り、受け取った部分コンテンツ$C4^{(n)}$を蓄積する。鍵埋込／抽出部2001は、コンテンツC4のヘッダ部分から装置記録鍵K_{HDD}を抽出し、抽出した装置記録鍵K_{HDD}を装置記録鍵記憶部202に書き込む。鍵埋込／抽出部2001は、装置記録鍵K_{HDD}を抽出した後のコンテンツC4を破棄する。

[0153] (2)暗号化／復号部2002

暗号化／復号部2002は、鍵埋込／抽出部2001から装置記録鍵K_{HDD}が埋め込まれたコンテンツC4を受け取ると、コンテンツC4を先頭から128ビット毎の部分コンテンツ$C4^{(n)}$に分割する。また、暗号化／復号部2002は、媒体記録鍵記憶部209から媒体記録鍵K_Tを読み出す。

[0154] 暗号化／復号部2002は、媒体記録鍵K_Tを暗号鍵として用い、部分コンテンツ$C4^{(n)}$を順次暗号化して、暗号化部分コンテンツ$EC4^{(n)}$を生成する。暗号化／復号部2002は、生成した暗号化部分コンテンツ$EC4^{(n)}$を書込／読出部213へ出力する。

また、暗号化／復号部2002は、書込／読出部213から暗号化コンテンツEC4及び媒体記録鍵K_Tを受け取ると、受け取った暗号化コンテンツEC4を、先頭から128ビット毎の暗号化部分コンテンツ$EC4^{(n)}$に分割する。暗号化／復号部2002は、媒体記録鍵K_Tを復号鍵として用い、暗号化部分コンテンツ$EC4^{(n)}$を復号して、部分コンテンツ$C4^{(n)}$を生成する。暗号化／復号部2002は、生成した部分コンテンツ$C4^{(n)}$を、鍵埋込／抽出部2001へ出力する。

[0155] ＜動作＞

1．システム全体

コンテンツ保護システム2全体の動作は、図7に示したフローチャートの「記録再生装置10」を「記録再生装置20」に置き換えればよい。

2．記録再生装置20から可搬媒体14へのコンテンツ利用権移動処理の動作

図18は、記録再生装置20から可搬媒体14へのコンテンツのムーブ処理の動作を示すフローチャートである。ここに示す動作は、「記録再生装置10」を「記録再生装置20」に置き換えた図7のステップS4の詳細である。

[0156] 記録再生装置20の媒体記録鍵生成部208は、媒体記録鍵K_Tを生成し（ステップS201）。生成した媒体記録鍵K_Tを、媒体記録鍵記憶部209に格納する。

次に、記録再生装置20は、記憶部204の暗号化コンテンツ領域に格納されている暗号化コンテンツEC2を、暗号化部分コンテンツ$EC2^{(n)}$に分割し、ステップS202からステップS205まで、n＝1，2，・・・，Mについて繰り返す。また、可搬媒体14は、ステップS211からステップS213まで、n＝1，2，・・・，Mについて繰り返す。

[0157] 先ず、記録再生装置20の復号部205は、暗号化部分コンテンツ$EC2^{(n)}$を、装置記録鍵K_{HDD}で復号し、部分コンテンツ$C2^{(n)}$を生成する（ステップS203）。次に、変換部207は、MPEG-2の部分コンテンツ$C2^{(n)}$をダウンコンして、MPEG-4の部分コンテンツ$C4^{(n)}$を生成する（ステップS204）。次に、鍵埋込／抽出部2001は、ステップS204で生成された部分コンテンツ$C4^{(n)}$を蓄積し、コンテンツC4を生成する（ステップS206）。鍵埋込／抽出部2001は、コンテンツC4のヘッダ部分に装置記録鍵K_{HDD}を埋め込む（ステップS207）。

[0158] 続いて、記録再生装置20は、ステップS208からステップS230までn＝1，2，・・・，

Mについて繰り返す。

暗号化／復号部2002は、鍵埋込／抽出部2001からコンテンツC4を受け取ると、受け取ったコンテンツC4の先頭から128ビット毎の部分コンテンツ$C4^{(n)}$に分割する。更に、暗号化／復号部2002は、媒体記録鍵記憶部209から媒体記録鍵K_Tを読み出す。

[0159] 暗号化／復号部2002は、媒体記録鍵K_Tを暗号鍵として用い、部分コンテンツ$C4^{(n)}$を暗号化して、暗号化部分コンテンツ$EC4^{(n)}$を生成する（ステップS209）。暗号化／復号部2002は、生成した暗号化部分コンテンツ$EC4^{(n)}$を、書込／読出部213へ出力する。

書込／読出部213は、暗号化部分コンテンツ$EC4^{(n)}$を、可搬媒体14に出力し、可搬媒体14の入出力部132は、暗号化部分コンテンツ$EC4^{(n)}$を受け取る（ステップS210）。可搬媒体14の記録制御部133は、入出力部141を介して暗号化部分コンテンツ$EC4^{(n)}$を受け取り、記憶部134の暗号化コンテンツ領域134aに書き込み、暗号化コンテンツ領域134aは、暗号化部分コンテンツ$EC4^{(n)}$を格納する（ステップS212）。

[0160] 記録再生装置20は、ステップS210の出力が終了すると、装置記録鍵記憶部202から装置記録鍵K_{HDD}を消去する（ステップS215）。次に、書込／読出部213は、記憶部204から機器ID「ID__A」を読み出す（ステップS216）。書込／読出部213は、読み出したID__Aを、可搬媒体14へ出力し、可搬媒体14の入出力部132は、ID__Aを受け取る（ステップS217）。

[0161] 可搬媒体14の記録制御部133は、ID__Aを受け取り、受け取ったID__Aを、記憶部134の所定の領域に書き込み、記憶部134は、ID__Aを格納する（ステップS218）。

次に、書込／読出部213は、媒体記録鍵記憶部209から媒体記録鍵K_Tを読み出し（ステップS219）、読み出した媒体記録鍵K_Tを、可搬媒体14へ出力し、可搬媒体14の入出力部132は、K_Tを受け取る（ステップS220）。

[0162] 可搬媒体14の記録制御部133は、媒体記録鍵K_Tを媒体記録鍵領域134bに書き込み、媒体記録鍵領域134bは、K_Tを格納する（ステップS221）。記録再生装置20は、ステップS220の出力が終了すると、媒体記録鍵記憶部209から、媒体記録鍵K

K_Tを消去する(ステップS222)。

可搬媒体14の記録制御部133は、媒体記録鍵K_Tを媒体記録鍵領域134bに書き込むと、機器ID領域134dからID_Bを読み出し(ステップS223)、入出力部132へ渡す。入出力部132は、ID_Bを記録再生装置20へ出力し、記録再生装置20の書込/読出部213は、ID_Bを受け取る(ステップS224)。

[0163] 書込/読出部213は、受け取ったID_Bを記録制御部215へ出力する。記録制御部215は、ID_Bを受け取ると、記憶部204に格納する(ステップS225)。

図19は、記録再生装置20から可搬媒体14へ、コンテンツをムーブする処理の過程において、記録再生装置20及び可搬媒体14のそれぞれが保持するデータを説明する図面である。

[0164] (a)は、コンテンツをムーブする以前の記録再生装置20及び可搬媒体14が保持するデータを示している。

記録再生装置20の記憶部204は、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部209は、媒体記録鍵K_Tを記憶している。装置記録鍵記憶部202は、装置記録鍵K_{HDD}を記憶している。

[0165] 可搬媒体14の暗号化コンテンツ領域134a及び媒体記録鍵領域134bは、何れもデータを保持していない。

このとき、記録再生装置20は、コンテンツ利用可能状態であり、MPEG-2コンテンツを利用できる。勿論、可搬媒体14は、コンテンツを保持しておらず、コンテンツ利用不可能状態である。

[0166] (b)は、暗号化コンテンツEC4の可搬媒体14への書き込みが終了した時点の記録再生装置20及び可搬媒体14が保持するデータを示している。

記録再生装置20の記憶部204は、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部209は、媒体記録鍵K_Tを記憶している。装置記録鍵記憶部202は、装置記録鍵K_{HDD}を記憶している。

[0167] 可搬媒体14の暗号化コンテンツ領域134aは、そのヘッダ部分に装置記録鍵K_{HDD}が埋め込まれた、MPEG-4の暗号化コンテンツを記憶している。ここでは、ヘッダ部分にK_{HDD}が埋め込まれていることから「(K_{HDD})EC4」と記載している。媒体記録鍵領

域134bは、データを保持していない。

このとき、記録再生装置20は、コンテンツ利用可能状態であり、MPEG-2コンテンツを利用できる。可搬媒体14は、暗号化されたMPEG-4コンテンツEC4とMPEG-4コンテンツに埋め込まれている装置記録鍵K_{HDD}とを保持しているが、暗号化を解く媒体記録鍵K_Tを保持していないため、コンテンツ利用不可能状態である。

[0168] (c)は、装置記録鍵K_{HDD}の可搬媒体14への移動が終了した時点の記録再生装置20及び可搬媒体14が保持するデータを示している。

記録再生装置20の記憶部204は、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部209は、媒体記録鍵K_Tを記憶している。装置記録鍵記憶部202は、データを保持していない。

[0169] 可搬媒体14の暗号化コンテンツ領域134aは、装置記録鍵K_{HDD}が埋め込まれたMPEG-4の暗号化コンテンツ(K_{HDD})EC4を記憶している。媒体記録鍵領域134bは、データを保持していない。

このとき、記録再生装置20は、暗号化されたMPEG-2コンテンツを保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。可搬媒体14は、暗号化されたMPEG-4コンテンツとMPEG-4コンテンツに埋め込まれた装置記録鍵K_{HDD}とを保持しているが、暗号化を解く媒体記録鍵K_Tを保持していないため、コンテンツ利用不可能状態である。

[0170] (d)は、コンテンツのムーブ処理が終了した時点の記録再生装置20及び可搬媒体14が保持するデータを示している。

記録再生装置20の記憶部204は、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部109及び装置記録鍵記憶部102は、何れもデータを保持していない。

[0171] 可搬媒体14の暗号化コンテンツ領域134aは、装置記録鍵K_{HDD}が埋め込まれたMPEG-4の暗号化コンテンツ(K_{HDD})EC4を記憶している。媒体記録鍵領域134bは、媒体記録鍵K_Tを記憶している。

このとき、記録再生装置20は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可

能状態である。一方、可搬媒体14は、装置記録鍵K_{HDD}が埋め込まれて暗号化されたMPEG-4コンテンツ(K_{HDD})EC4及び暗号化を解くための媒体記録鍵K_Tを保持しているため、コンテンツ利用可能状態である。

[0172] 3. 可搬媒体14から記録再生装置20へのコンテンツ利用権移動処理の動作

図20は、可搬媒体14から記録再生装置20へのコンテンツのムーブ処理の動作を示すフローチャートである。ここに示す動作は、「記録再生装置10」を「記録再生装置20」に置き換えた図7のステップS7の詳細である。

可搬媒体14の記録制御部133は、記憶部134の所定の領域から、ステップS218で格納した機器ID[ID__A]を読み出し(ステップS241)、読み出した機器ID「ID__A」を、入出力部132を介して記録再生装置20へ出力し、記録再生装置20の書込／読出部213は、機器ID「ID__A」を受け取る(ステップS242)。

[0173] 書込／読出部213は、記憶部204から機器IDを読み出し、読み出した機器IDと、ステップS242で受け取った機器ID「ID__A」とが一致するか否か判断する(ステップS243)。一致しない場合(ステップS244でNO)、書込／読出部213は、受け取った機器ID「ID__A」を破棄し、エラーである旨をモニタ12へ出力するなど、エラー処理を行う(ステップS245)。一致する場合(ステップS244でYES)、処理を続ける。

[0174] 可搬媒体14の記録制御部133は、媒体記録鍵領域134bから媒体記録鍵K_Tを読み出し(ステップS246)、読み出した媒体記録鍵K_Tを、入出力部132を介して書込／読出部213へ出力し、書込／読出部213は、K_Tを受け取る(ステップS247)。書込／読出部213は、媒体記録鍵K_Tを暗号化／復号部2002へ出力し、暗号化／復号部2002は、媒体記録鍵K_Tを内部に格納する(ステップS248)。

[0175] ステップS247において、K_Tの出力が終了すると、記録制御部133は、媒体記録鍵領域134bから媒体記録鍵K_Tを消去する(ステップS249)。次に、記録制御部133は、暗号化コンテンツ領域134aから、ヘッダ部分にK_{HDD}を含む暗号化コンテンツEC4を読み出し(ステップS250)、入出力部132を介して、書込／読出部213へ出力し、書込／読出部213は、EC4を受け取る(ステップS251)。

[0176] 書込／読出部213は、受け取った暗号化コンテンツEC4を、暗号化／復号部2002へ出力し、暗号化／復号部2002は、暗号化コンテンツEC4を、内部に格納する(

ステップS252)。

暗号化／復号部2002は、暗号化コンテンツEC4を先頭から128ビット毎に、暗号化部分コンテンツ$EC4^{(n)}$に分割し、ステップS253からステップS255までn＝1，2，・・・，Mについて繰り返す。暗号化／復号部2002は、媒体記録鍵K_Tを復号鍵として用い、暗号化部分コンテンツ$EC4^{(n)}$を復号し、部分コンテンツ$C4^{(n)}$を生成する(ステップS254)。暗号化／復号部2002は、生成した部分コンテンツ$C4^{(n)}$を、鍵埋込／抽出部2001へ出力し、鍵埋込／抽出部2001は、部分コンテンツ$C4^{(n)}$を蓄積する。

[0177] 鍵埋込／抽出部2001は、部分コンテンツ$C4^{(n)}$を蓄積して成るコンテンツC4のヘッダ部分から、装置記録鍵K_{HDD}を抽出する(ステップS256)。鍵埋込／抽出部2001は、装置記録鍵K_{HDD}を抽出した後のコンテンツC4を破棄する(ステップS257)。

鍵埋込／抽出部2001は、抽出した装置記録鍵K_{HDD}を、装置記録鍵記憶部202へ書き込み、装置記録鍵記憶部202は、装置記録鍵K_{HDD}を格納する(ステップS258)。

[0178] 図21は、可搬媒体14から記録再生装置20へ、コンテンツをムーブする処理の過程において、記録再生装置20及び可搬媒体14のそれぞれが保持するデータを説明する図面である。

(a)は、コンテンツをムーブする以前の記録再生装置20及び可搬媒体14が保持するデータを示しており、図19(d)に示した状態と同一である。即ち、記録再生装置20は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。一方、可搬媒体14は、暗号化されたMPEG-4コンテンツEC4及び暗号化を解くための媒体記録鍵K_Tを保持しているため、コンテンツ利用可能状態である。

[0179] (b)は、暗号化コンテンツEC4及び媒体記録鍵K_Tを、可搬媒体14から記録再生装置20へ移動させた時点の記録再生装置20及び可搬媒体14が保持するデータを示している。

記録再生装置20の記憶部204は、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部209及び装置記録鍵記憶部202は、何れもデータを保持していない。

[0180] 可搬媒体14の暗号化コンテンツ領域134a及び媒体記録鍵領域134bは、何れもデータを保持していない。

このとき、記録再生装置20は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解く装置記録鍵K_{HDD}を保持していないため、コンテンツ利用不可能状態である。可搬媒体14は、勿論コンテンツを利用不可能状態である。

[0181] (c)は、コンテンツのムーブが終了した時点の記録再生装置20及び可搬媒体14が保持するデータを示している。

記録再生装置20の記憶部204は、MPEG-2の暗号化コンテンツEC2を記憶している。媒体記録鍵記憶部209は、データを保持していない。装置記録鍵記憶部102は、装置記録鍵K_{HDD}を記憶している。

[0182] 可搬媒体14の暗号化コンテンツ領域134a、媒体記録鍵領域134b及び暗号化装置記録鍵領域134cは、何れもデータを保持していない。

このとき、記録再生装置10は、コンテンツ利用可能状態であり、高画質なMPEG-2コンテンツを利用できる。可搬媒体14は、コンテンツを保持しておらず、コンテンツ利用不可能状態である。

＜実施例3＞

本発明における第3の実施例として、コンテンツ保護システム3について説明する。

[0183] ＜構成＞

1. システム全体

図22は、コンテンツ保護システム3の構成、更には、記録再生装置30の機能的な構成を示す図である。同図に示す様に、コンテンツ保護システム3は、記録再生装置30、コンテンツ供給装置11、モニタ12、スピーカ13、可搬媒体14及び携帯情報端末15から構成される。

[0184] コンテンツ保護システム3は、コンテンツ保護システム1と同様に、放送局に設置されたコンテンツ供給装置11から放送されるデジタル放送番組であるコンテンツを、記録再生装置30が受信し、受信したコンテンツを記録及び再生し、また、記録再生装置30に記録されているコンテンツを可搬媒体14へムーブし、ムーブされたコンテンツを、携帯情報端末15により再生する。更に、可搬媒体14に記録されているコンテン

ツを再度記録再生装置30へムーブするシステムである。

[0185] コンテンツ供給装置11及び携帯情報端末15は、それぞれ、コンテンツ保護システム1における装置と同一の機能及び構成を有する。

なお、図14に示した可搬媒体14は、入出力部132、記録制御部133、機器ID領域134dを省略している。コンテンツ保護システム3における可搬媒体14は、媒体記録鍵領域134b及び装置記録鍵領域134cを備えず、コンテンツ鍵領域3002を備える。

[0186] 以下では、特に、コンテンツ保護システム1との相違点である記録再生装置30について説明する。

2. 記録再生装置30

図22に示す様に、記録再生装置30は、コンテンツ受信部301、暗号化部303、記憶部304、復号部305、再生部306、変換部307、暗号化部310、書込／読出部313、入力部314、記録制御部315及びコンテンツ鍵記憶部3001から構成される。

[0187] 図2に示した記録再生装置10との相違は、記録再生装置30は、媒体記録鍵生成部108、媒体記録鍵記憶部109、装置固有鍵記憶部111及び暗号化／復号部112に相当する構成要素を備えず、装置記録鍵記憶部102に替わって、コンテンツ鍵記憶部3001を備える点である。

コンテンツ受信部301、暗号化部303、記憶部304、復号部305、再生部306、変換部307、書込／読出部313、入力部314及び記録制御部315は、図1に示したコンテンツ受信部101、暗号化部103、記憶部104、復号部105、再生部106、変換部107、書込／読出部113、入力部114及び記録制御部115と同様の構成及び機能を有する。

[0188] コンテンツ鍵記憶部3001は、予め内部にコンテンツ鍵K_cを格納している。コンテンツ鍵K_cは、暗号化部303におけるMPEG-2コンテンツC2の暗号化、復号部305によるMPEG-2暗号化コンテンツEC2の復号、及び、暗号化部310によるMPEG-4コンテンツの暗号化の各処理において、暗号鍵及び復号鍵として用いられる128ビットの鍵データである。

[0189] 即ち、実施例1及び実施例2において、C2の暗号化及びEC2の復号処理におい

て、鍵データとして用いられる装置記録鍵K_{HDD}と、C4の暗号化処理に用いられる媒体記録鍵K_Tとを、同一のコンテンツ鍵K_Cにより実現する構成が、実施例3の特徴である。

＜動作＞

1. システム全体

コンテンツ保護システム3全体の動作は、図7に示したフローチャートの「記録再生装置10」を「記録再生装置30」に置き換えればよい。

[0190] 2. 記録再生装置30から可搬媒体14へのコンテンツ利用権移動処理の動作

図23は、記録再生装置30から可搬媒体14へのコンテンツのムーブ処理の動作を示すフローチャートである。ここに示す動作は、「記録再生装置10」を「記録再生装置30」に置き換えた図7のステップS4の詳細である。

記録再生装置30の暗号化部303は、コンテンツ鍵記憶部3001からコンテンツ鍵K_Cを読み出す（ステップS301）。また、暗号化部303は、記憶部304から暗号化コンテンツEC2を読み出し、読み出したEC2を暗号化部分コンテンツ$EC2^{(n)}$に分割し、ステップS302からステップS306まで、n＝1，2，・・・，Mについて繰り返す。

[0191] 先ず、記録再生装置30の復号部305は、暗号化部分コンテンツ$EC2^{(n)}$を、コンテンツ鍵K_Cで復号し、部分コンテンツ$C2^{(n)}$を生成する（ステップS303）。次に、変換部307は、MPEG-2の部分コンテンツ$C2^{(n)}$をダウンコンして、MPEG-4の部分コンテンツ$C4^{(n)}$を生成する（ステップS304）。

暗号化部310は、コンテンツ鍵記憶部3001から、コンテンツ鍵K_Cを読み出し、コンテンツ鍵K_Cを暗号鍵として用い、部分コンテンツ$C4^{(n)}$を暗号化して、暗号化部分コンテンツ$EC4^{(n)}$を生成する（ステップS305）。暗号化部310は、生成した暗号化部分コンテンツ$EC4^{(n)}$を蓄積しておく。

[0192] 次に、書込／読出部313は、コンテンツ鍵記憶部302からコンテンツ鍵K_Cを読み出し、更に、記憶部304から機器ID「ID__A」を読み出す（ステップS307）。書込／読出部313は、読み出したコンテンツ鍵K_C及び機器ID「ID__A」を、可搬媒体14へ出力し、可搬媒体14の入出力部132は、コンテンツ鍵K_C及び機器ID「ID__A」を受け取る（ステップS308）。

[0193] 可搬媒体14の記録制御部133は、コンテンツ鍵K_C及び機器ID「ID__A」を受け取り、受け取ったコンテンツ鍵K_Cを、コンテンツ鍵領域3002へ書き込み、コンテンツ鍵領域3002は、コンテンツ鍵K_Cを格納する。また、記録制御部133は、機器ID「ID__A」を、記憶部134の所定の領域に書き込む(ステップS309)。

記録再生装置30は、ステップS308によるコンテンツ鍵K_Cの出力が終了すると、コンテンツ鍵記憶部3001からコンテンツ鍵K_Cを消去する(ステップS310)。

[0194] 次に、書込／読出部313は、暗号化部310に蓄積されている暗号化コンテンツEC4を読み出し(ステップS311)、読み出した暗号化コンテンツEC4を、可搬媒体14に出力し、可搬媒体14の入出力部132は、暗号化コンテンツEC4を受け取る(ステップS312)。可搬媒体14の記録制御部133は、入出力部132を介して暗号化コンテンツEC4を受け取り、暗号化コンテンツ領域134aに格納する(ステップS313)。

[0195] 暗号化コンテンツEC4を格納すると、記録制御部133は、機器ID領域134dからID__Bを読み出し(ステップS314)、入出力部132へ渡す。入出力部132は、ID__Bを記録再生装置30へ出力し、記録再生装置30の書込／読出部313は、ID__Bを受け取る(ステップS315)。

書込／読出部313は、受け取ったID__Bを記録制御部315へ出力する。記録制御部315は、ID__Bを受け取ると、記憶部304に格納する(ステップS316)。

[0196] 図24は、記録再生装置30から可搬媒体14へ、コンテンツをムーブする処理の過程において、記録再生装置30及び可搬媒体14のそれぞれが保持するデータを説明する図面である。

(a)は、コンテンツをムーブする以前の記録再生装置30及び可搬媒体14が保持するデータを示している。

[0197] 記録再生装置30の記憶部304は、MPEG-2の暗号化コンテンツEC2を記憶している。コンテンツ鍵記憶部3001は、コンテンツ鍵K_Cを記憶している。

可搬媒体14の暗号化コンテンツ領域134a及びコンテンツ鍵領域3002は、何れもデータを保持していない。

このとき、記録再生装置20は、コンテンツ利用可能状態であり、MPEG-2コンテンツを利用できる。可搬媒体14は、コンテンツを保持しておらず、コンテンツ利用不可

能状態である。

[0198] (b)は、コンテンツ鍵K_cの移動が終了した時点の記録再生装置30及び可搬媒体14が保持するデータを示している。

記録再生装置30の記憶部304は、MPEG-2の暗号化コンテンツEC2を記憶している。コンテンツ鍵記憶部3001は、データを保持していない。

可搬媒体14の暗号化コンテンツ領域134aは、データを保持していない。コンテンツ鍵領域3002は、コンテンツ鍵K_cを記憶している。

[0199] このとき、記録再生装置30は、暗号化コンテンツEC2は保持しているが、暗号化を解くためのコンテンツ鍵K_cを保持していないため、コンテンツ利用不可能状態である。可搬媒体14は、コンテンツ鍵K_cを保持しているが、暗号化コンテンツ自体を保持していないため、コンテンツ利用不可能状態である。

(c)は、コンテンツのムーブ処理が終了した時点の記録再生装置30及び可搬媒体14が保持するデータを示している。

[0200] 記録再生装置30の記憶部304は、MPEG-2の暗号化コンテンツEC2を記憶している。コンテンツ鍵記憶部3001は、データを保持していない。

可搬媒体14の暗号化コンテンツ領域134aは、MPEG-4の暗号化コンテンツEC4を記憶している。コンテンツ鍵領域3002は、コンテンツ鍵K_cを記憶している。

このとき、記録再生装置30は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解くコンテンツ鍵K_cを保持していないため、コンテンツ利用不可能状態である。一方、可搬媒体14は、暗号化されたMPEG-4コンテンツEC4及び暗号化を解くためのコンテンツ鍵K_cを保持しているため、コンテンツ利用可能状態である。

[0201] 3. 可搬媒体14から記録再生装置30へのコンテンツ利用権移動処理の動作

図25は、可搬媒体14から記録再生装置30へのコンテンツのムーブ処理の動作を示すフローチャートである。ここに示す動作は、「記録再生装置10」を「記録再生装置30」に置き換えた図7のステップS7の詳細である。

可搬媒体14の記録制御部133は、暗号化コンテンツ領域134aから、暗号化コンテンツEC4を消去する(ステップS331)。次に、記録制御部133は、コンテンツ鍵領域

3002から、コンテンツ鍵K_Cを読み出し、また所定の領域から機器ID「ID__A」を読み出す(ステップS332)。

[0202] コンテンツ鍵K_C及び機器ID「ID__A」は、入出力部132を介して、記録再生装置30へ出力され、記録再生装置30の書込／読出部313は、コンテンツ鍵K_C及び機器ID「ID__A」を受け取る(ステップS334)。書込／読出部313は、受け取った機器ID「ID__A」が、自機の機器IDと一致するか否か確認する(ステップS335)。一致しない場合(ステップS336でNO)、書込／読出部313は、受け取った機器ID「ID__A」とコンテンツ鍵K とを破棄する。その後、記録再生装置30は、エラーである旨をモニタ12に出力する等、エラー処理を行う(ステップS337)。

[0203] 受け取った機器ID「ID__A」が、自機の機器IDと一致する場合(ステップS336でYES)、書込／読出部313は、コンテンツ鍵K_Cを、コンテンツ鍵記憶部3001へ書き込み、コンテンツ鍵記憶部3001は、コンテンツ鍵K_Cを格納する(ステップS338)。

可搬媒体14の記録制御部133は、コンテンツ鍵K_Cがコンテンツ鍵記憶部3001に格納されると、コンテンツ鍵領域3002に格納されているコンテンツ鍵K_Cを消去し(ステップS339)、更に、所定の領域に格納されている機器ID「ID__A」を消去する(ステップS340)。

[0204] 図26は、可搬媒体14から記録再生装置30へ、コンテンツをムーブする処理の過程において、記録再生装置30及び可搬媒体14のそれぞれが保持するデータを説明する図面である。

(a)は、コンテンツをムーブする以前の記録再生装置30及び可搬媒体14が保持するデータを示しており、図24(c)に示した状態と同一である。即ち、記録再生装置30は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解くコンテンツ鍵K_Cを保持していないため、コンテンツ利用不可能状態である。一方、可搬媒体14は、暗号化されたMPEG-4コンテンツEC4及び暗号化を解くためのコンテンツ鍵K_Cを保持しているため、コンテンツ利用可能状態である。

[0205] (b)は、暗号化コンテンツEC4の消去が終了した時点の記録再生装置30及び可搬媒体14が保持するデータを示している。

記録再生装置30の記憶部304は、暗号化されたMPEG-2コンテンツEC2を記憶

している。コンテンツ鍵記憶部3001は、データを保持していない。

可搬媒体14の暗号化コンテンツ領域134aは、データを保持していない。コンテンツ鍵領域3002は、コンテンツ鍵K_cを保持している。

[0206] このとき、記録再生装置30は、暗号化されたMPEG-2コンテンツEC2を保持しているが、暗号化を解くコンテンツ鍵K_cを保持していないため、コンテンツ利用不可能状態である。可搬媒体14は、コンテンツ鍵K_cを保持しているが、コンテンツ自体を保持していないため、勿論コンテンツを利用不可能状態である。

(c)は、コンテンツのムーブが終了した時点の記録再生装置30及び可搬媒体14が保持するデータを示している。

[0207] 記録再生装置30の記憶部304は、MPEG-2の暗号化コンテンツEC2を記憶している。コンテンツ鍵記憶部3001は、コンテンツ鍵K_cを記憶している。

可搬媒体14の暗号化コンテンツ領域134a及びコンテンツ鍵領域3002は、何れもデータを保持していない。

このとき、記録再生装置10は、コンテンツ利用可能状態であり、高画質なMPEG-2コンテンツを利用できる。可搬媒体14は、コンテンツを保持しておらず、コンテンツ利用不可能状態である。

＜実施例4＞

以下では、本発明の他の実施形態について、図面を参照しながら説明する。図27は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツを供給するコンテンツ供給装置1101と、前記コンテンツを獲得して、コンテンツの記録、並びに再生を行い、さらにコンテンツの移動を実行する記録再生装置1102と、前記移動するコンテンツを獲得する記録再生装置1103、あるいは可搬媒体1104からなる。

[0208] 記録再生装置1102は、コンテンツ供給装置1101からコンテンツを受信して記録する際、当該コンテンツを暗号化して、例えば内蔵HDDに記録する。そして、当該コンテンツを移動する際は、移動先となる装置、あるいは可搬媒体が正規装置、あるいは正規可搬媒体であるか否かを確認(認証)した上で、コンテンツの移動を実行する。さらに、記録再生装置1102は、コンテンツの移動が完了した後に、内部に記録す

るコンテンツを利用できない状態にする。ここで、認証技術は、例えば、相手が装置であれば、DTCP規格で定められた手順を用いることができ、相手が可搬媒体であればCPRM SD(Content Protection for Recordable Media Specification SD Memory Card Book)規格で定められた手順を用いることができる。あるいは、非特許文献1、並びに非特許文献2に開示される公知の任意の技術を用いることができる。このように認証技術は、公知の技術で実現可能なため、その詳細についてはここでは言及しない。

[0209] 図28は、本発明の実施例4における、記録再生装置1102がコンテンツを記録、並びに再生を行い、さらに記録再生装置1102から可搬媒体1104にコンテンツを移動させる場合の記録再生装置1102、並びに可搬媒体1104の機能を示す機能ブロック図である。

記録再生装置1102は、外部からコピー制御情報と、コンテンツを受信する受信部1201と、前記コピー制御情報に基づき、前記受信したコンテンツを記録再生装置1102(具体的には、後述する暗号化コンテンツ記録部1210、211)に記録することが認められているか否かを判定する判定部1202と、前記コピー制御情報を、必要に応じて更新した後、記録するコピー制御情報記録部1204と、前記受信したコンテンツを暗号化するために用いるコンテンツ鍵を生成する鍵生成部1205と、前記生成したコンテンツ鍵を記録するコンテンツ鍵記録部1206と、コンテンツ鍵記録部1206に記録したコンテンツ鍵へのアクセスを制御する制御部1203と、前記コンテンツ鍵を用いて、前記受信したコンテンツを暗号化して、第1暗号化コンテンツを生成する暗号化部1208と、前記第1暗号化コンテンツを記録する暗号化コンテンツ記録部1210と、前記受信したコンテンツを、変換する変換部1207と、前記コンテンツ鍵を用いて、前記変換したコンテンツを暗号化して第2暗号化コンテンツを生成する暗号化部1209と、前記第2暗号化コンテンツを記録する暗号化コンテンツ記録部1211とを備える。

[0210] また、記録再生装置1102は、さらに、前記第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを、前記コンテンツ鍵を用いて復号化する復号化部1221と、復号した第1暗号化コンテンツ、もしくは、復号した第2暗号化コンテンツを再生する再生部1222と、コピー制御情報記録部1204に記録したコピー制御情報に基づいて、暗号

化コンテンツ記録部1211に記録した第2暗号化コンテンツを、記録再生装置1102から可搬媒体1104に移動することが認められているか否か判定する、もしくは、後述する可搬媒体1104のコピー制御情報記録部1216に記録したコピー制御情報に基づいて、可搬媒体1104の暗号化コンテンツ記録部1218に記録した第2暗号化コンテンツを、可搬媒体1104から記録再生装置1102に移動することが認められているか否か判定する判定部1212と記録再生装置1102と可搬媒体1104との間で、相互に、相手が正当であるか否かを認証する認証部1223、認証が成功した時に、記録再生装置1102と可搬媒体1104との間で、やり取りされるコンテンツ鍵、及び、コピー制御情報を暗号化、復号化するための暗号化／復号化部1225、コピー制御情報記録部1204に記録したコピー制御情報、コンテンツ鍵記録部1206に記録したコンテンツ鍵、並びに、暗号化コンテンツ記録部1211に記録した第2暗号化コンテンツを可搬媒体1104に書き込む、もしくは、可搬媒体1104から読み出す書込／読出部1213とを備える。

[0211] 記録再生装置1102が備える制御部1203、コピー制御情報記録部1204、並びに、コンテンツ鍵記録部1206は、外部からのデータの読み書きが不可能なセキュアな領域1214に設けられる。この領域1214は、具体的には、耐タンパハードウエア、耐タンパソフトウエア、あるいは、両者の組み合わせで構成する。暗号化コンテンツ記録部1210、211は、外部からの読み書きが可能な領域1215に設けられる。この領域1215は、例えば、HDD（Hard Disk Drive）により構成する。

[0212] 一方、可搬媒体1104は、記録再生装置1102と可搬媒体1104との間で、相互に、相手が正当であるか否かを認証する認証部1224と、認証が成功した時に、記録再生装置1102と可搬媒体1104との間で、やり取りされるコンテンツ鍵、及び、コピー制御情報を暗号化、復号化するための暗号化／復号化部1226とを備える。

また、可搬媒体1104は、さらに、前記第2暗号化コンテンツを記録する暗号化コンテンツ記録部1218と、前記コンテンツ鍵を記録するコンテンツ鍵記録部1217と、前記コピー制御情報を記録するコピー制御情報記録部1216を備える。可搬媒体1104が備えるコピー制御情報記録部1216、並びに、コンテンツ鍵記録部1217は、外部から正当な装置以外読み書きできない領域1219に設けられる。この領域1219は

、可搬媒体1104の認証部1224と、記録再生装置1102の認証部1223との間で、認証処理が正しく実行できた場合のみ、記録再生装置1102からのデータの読み書きが可能となる領域である。暗号化コンテンツ記録部1218は、外部からの読み書きが可能な領域1220に設けられる。

[0213] 次に、図29を用いて、受信したコンテンツを記録再生装置1102に記録する場合の動作について説明する。

S501:記録再生装置1102の受信部1201は、コンテンツとコピー制御情報を受信する。

S502:判定部1202は、「前記コピー制御情報が、受信したコンテンツを記録再生装置1102に記録することが認められているか否か」を判定する。判定の結果、「記録は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「記録は認められる」と判定した場合は、以降の処理を実行する。

[0214] S503:前記コピー制御情報を、必要に応じて更新してコピー制御情報記録部1204に記録する。

S504:鍵生成部1205は、コンテンツ鍵を生成し、コンテンツ鍵記録部1206に記録する。

S505:暗号化部1208は、受信したコンテンツを、コンテンツ鍵記録部1206に記録しているコンテンツ鍵で暗号化して第1暗号化コンテンツを生成する。

[0215] S506:前記第1暗号化コンテンツを暗号化コンテンツ記録部1210に記録する。

S507:変換部1207は、受信したコンテンツを、変換する。

S508:暗号化部1209は、前記変換したコンテンツを、コンテンツ鍵記録部1206に記録しているコンテンツ鍵で暗号化して第2暗号化コンテンツを生成する。

S509:前記第2暗号化コンテンツを暗号化コンテンツ記録部1211に記録する。

[0216] ここで、コピー制御情報としては、例えば、コピーが禁止されていることを示す「Copy Never」や、コピーが1回だけ許されていることを示す「Copy One Generation」などが用いられる。この場合、判定部1202は、コピー制御情報が「Copy Never」であれば、「記録は認められない」と判定し、コピー制御情報が「Copy One Generation」であれば、「記録は認められている」と判定する。後者の場合、コンテンツを記

録再生装置に記録するのに伴い、コピー制御情報は、「Copy One Generation」から、コピー禁止を示す「No More Copy」へ更新してコピー制御情報記録部1204に記録する。

[0217] 変換部1207は、例えば、受信したコンテンツが、MPEG2形式の映像コンテンツである場合に、MPEG4形式の映像コンテンツに変換する。

次に、図30を用いて、記録再生装置1102から、可搬媒体1104へコンテンツを移動する場合の動作について説明する。

S401:記録再生装置1102の判定部1212は、書込／読出部1213を介して、コピー制御情報記録部1204に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部1211に記録した第2暗号化コンテンツを可搬媒体1104に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

[0218] S402:記録再生装置104の認証部1223は、可搬媒体1104の認証部1224との間で相互認証を行い、相互認証が成功した時は、認証部1223、224はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

S403:書込／読出部1213は、コピー制御情報記録部1204に記録しているコピー制御情報、並びに、コンテンツ鍵記録部1206に記録しているコンテンツ鍵を読み出す。

[0219] このとき、制御部1203は、コンテンツ鍵記録部1206に記録しているコンテンツ鍵が、以降、アクセスできないように利用不可状態にする。

S404:書込／読出部1213は、読み出したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部1225にて、前記セッション鍵を用いて暗号化して可搬媒体1104に送り、可搬媒体1104は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部1226にて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、コンテンツ鍵を可搬媒体1104に記録する。

[0220] S405:コピー制御情報記録部1204に記録しているコピー制御情報と、コンテンツ

鍵記録部1206に記録しているコンテンツ鍵を消去する。

S406:書込／読出部1213は、暗号化コンテンツ記録部1211に記録している第2暗号化コンテンツを読出す。

S407:読み出した第2暗号化コンテンツを可搬媒体1104に記録する。

[0221] S408:暗号化コンテンツ記録部1211に記録している第2暗号化コンテンツを消去する。

図30、図31は、上記動作における記録再生装置1102、並びに可搬媒体1104における各データの記録状態を示した図である。図30(a)は、上記ステップS401の開始時点、(b)は、上記ステップS403の終了時点、(c)は、ステップS404の終了時点、(d)は、ステップS405の終了時点、図31(e)は、ステップS407の終了時点、(f)は、ステップS408の終了時点である。

[0222] ここで、ステップS403において、制御部1203は、コンテンツ鍵記録部1206に記録しているコンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。これにより、ステップS404が終了し、ステップS405が開始する前のタイミングで(図30(c))、電源断、もしくは、可搬媒体1104を記録再生装置1102から不正に引き抜く事などが行われたとしても、記録再生装置1102と、可搬媒体1104の両方において同時にコンテンツ鍵が利用可能な状態で存在することを防止できる。また、図30(a)ー図31(f)のどのタイミングで電源断が起こっても、記録再生装置1102と、可搬媒体1104のいずれかにおいてコンテンツ鍵は存在するため、移動元と移動先の両方でコンテンツ鍵が共に損なわれコンテンツが利用できなくなることはない。

[0223] ステップS402における認証部1223、224で実行される相互認証、及び、セッション鍵共有方法としては、例えば、チャレンジ—レスポンス型の相互認証、セッション鍵共有方法を用いる。チャレンジ—レスポンス型の相互認証、セッション鍵共有方法については、公知であるので説明は省略する。

次に、図32を用いて、可搬媒体1104から、記録再生装置1102へコンテンツを移動する場合の動作について説明する。

[0224] S601:記録再生装置1102の判定部1212は、書込／読出部1213を介して、可搬媒体1104のコピー制御情報記録部1216に記録されているコピー制御情報を受け

取り、「受け取ったコピー制御情報が、可搬媒体1104の暗号化コンテンツ記録部1218に記録した第2暗号化コンテンツを記録再生装置1102に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

[0225] S602:記録再生装置104の認証部1223は、可搬媒体1104の認証部1224との間で相互認証を行い、相互認証が成功した時は、認証部1223、224はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

S603:書込／読出部1213は、可搬媒体1104のコピー制御情報記録部1216に記録しているコピー制御情報、並びに、コンテンツ鍵記録部1217に記録しているコンテンツ鍵を読み出す。このとき、可搬媒体1104の暗号化／復号化部1226にて、コピー制御情報、並びに、コンテンツ鍵は、前記セッション鍵を用いて暗号化して、記録再生装置1102に送り、記録再生装置1102の暗号化／復号化部1225は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、前記セッション鍵を用いて復号して、書込／読出部1213に送る。

[0226] S604:書込／読出部1213は、読み出したコピー制御情報、並びに、コンテンツ鍵を、記録再生装置1102のコピー制御情報記録部1204、並びに、コンテンツ鍵記録部1206にそれぞれ記録する。このとき、制御部223は、コンテンツ鍵記録部1206に記録したコンテンツ鍵はアクセスできないよう利用不可状態にする。

S605:可搬媒体1104のコピー制御情報記録部1216に記録しているコピー制御情報、並びに、コンテンツ鍵記録部1217に記録しているコンテンツ鍵を消去する。

[0227] 制御部223は、コンテンツ鍵記録部1206に記録したコンテンツ鍵がアクセスできるように利用可能状態にする。

S606:書込／読出部1213は、可搬媒体1104の暗号化コンテンツ記録部1218に記録している第2暗号化コンテンツを読出す。

S607:読み出した第2暗号化コンテンツを記録再生装置1102の暗号化コンテンツ記録部1211に記録する。

[0228] S608：可搬媒体1104の暗号化コンテンツ記録部1218に記録している第2暗号化コンテンツを消去する。

図33、図34は、上記動作における記録再生装置1102、並びに可搬媒体1104における各データの記録状態を示した図である。図33(a)は、上記ステップS601の開始時点、(b)は、上記ステップS604の終了時点、(c)は、ステップS605の終了時点、(d)は、ステップS607の終了時点、図34(e)は、ステップS608の終了時点である。

[0229] 次に、図35を用いて、記録再生装置1102において、記録した第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを再生する場合の動作について説明する。

S801：復号化部1221は、暗号化コンテンツ記録部1210、もしくは、暗号化コンテンツ記録部1211より、第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを読出す。

[0230] S802：復号化部1221は、コンテンツ鍵記録部1206より、コンテンツ鍵を読み出す。

このとき、制御部1203は、コンテンツ鍵記録部1206に記録しているコンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。

S803：復号化部1221は、読み出した第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを、読み出したコンテンツ鍵を用いて復号化する。

[0231] S804：再生部1222は、復号した第1暗号化コンテンツもしくは、第2暗号化コンテンツを再生する。再生が終了すると、コンテンツ鍵記録部1206に記録しているコンテンツ鍵を利用可能状態にする。

ここで、ステップS802において、制御部1203により、コンテンツ鍵はアクセスできない利用不可状態にされるので、第1暗号化コンテンツの復号及び再生処理と、第2暗号化コンテンツの復号及び再生処理は、排他的にしか実行できない。

[0232] ＜変形例＞

実施例4では、第2暗号化コンテンツが記録再生装置1102から可搬媒体1104に移動する場合において、記録再生装置1102の制御部1203が、コンテンツ鍵が読み出されたときアクセスできないように利用不可状態にしたが、この構成に変えて、可

搬媒体1104の領域1219に制御部を設けても良い。この場合、第2暗号化コンテンツが記録再生装置1102から可搬媒体1104に移動する場合の動作は次の通りである。

[0233] S401：記録再生装置1102の判定部1212は、書込／読出部1213を介して、コピー制御情報記録部1204に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部1211に記録した第2暗号化コンテンツを可搬媒体1104に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

[0234] S402：記録再生装置104の認証部1223は、可搬媒体1104の認証部1224との間で相互認証を行い、相互認証が成功した時は、認証部1223、224はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

S403：書込／読出部1213は、コピー制御情報記録部1204に記録しているコピー制御情報、並びに、コンテンツ鍵記録部1206に記録しているコンテンツ鍵を読み出す。

[0235] S404：書込／読出部1213は、読み出したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部1225にて、前記セッション鍵を用いて暗号化して可搬媒体1104に送り、可搬媒体1104は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部1226にて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、コンテンツ鍵を可搬媒体1104に記録する。

[0236] このとき、可搬媒体の制御部は、可搬媒体1104のコンテンツ鍵記録部1217に記録しているコンテンツ鍵が、アクセスできないように利用不可状態にする。

S405：コピー制御情報記録部1204に記録しているコピー制御情報、並びに、コンテンツ鍵記録部1206に記録しているコンテンツ鍵を消去する。

このとき、可搬媒体1104の制御部は、コンテンツ鍵記録部1217に記録しているコンテンツ鍵が、アクセスできるように利用可能状態にする。

[0237] S406：書込／読出部1213は、暗号化コンテンツ記録部1211に記録している第2

暗号化コンテンツを読出す。

S407：読み出した第2暗号化コンテンツを可搬媒体1104に記録する。

S408：暗号化コンテンツ記録部1211に記録している第2暗号化コンテンツを消去する。

[0238] 同様に、実施例4では、第2暗号化コンテンツが可搬媒体1104から記録再生装置1102に移動する場合において、記録再生装置1102の制御部1203が、コンテンツ鍵が読み出されたときアクセスできないように利用不可状態にしたが、この構成に変えて、可搬媒体1104の領域1219に制御部を設けても良い。この場合の動作については、上記ステップS401からS408と同様であるので説明は省略する。

[0239] また、実施例4では、記録再生装置1102に制御部1203を設ける構成としたが、記録再生装置1102と、可搬媒体1104の双方に、制御部を設ける構成としてもよい。

以上、本発明の実施例4では、受信したコンテンツと、それを変換したコンテンツとを、それぞれ、同一のコンテンツ鍵を用いて、暗号化する構成について説明したが、この構成に限定されない。すなわち、受信したコンテンツと、それを変換したコンテンツとを、異なるコンテンツ鍵を用いて、暗号化する構成としてもよい。この場合について、以下、実施例5として説明する。

＜実施例5＞

図36は、本発明の実施例5における、記録再生装置1102aがコンテンツを記録、並びに再生を行い、さらに記録再生装置1102aから可搬媒体1104aにコンテンツを移動させる場合の記録再生装置1102a、並びに可搬媒体1104aの機能を示す機能ブロック図である。

[0240] 記録再生装置1102aは、外部からコピー制御情報と、コンテンツを受信する受信部1201aと、前記コピー制御情報に基づき、前記受信したコンテンツを記録再生装置1102a（具体的には、後述する暗号化コンテンツ記録部1210a、211a）に記録することが認められているか否かを判定する判定部1202aと、前記コピー制御情報を、必要に応じて更新した後、記録するコピー制御情報記録部1204aと、前記受信したコンテンツを暗号化するために用いる第1コンテンツ鍵と、第2コンテンツ鍵を生成する鍵生成部1205aと、前記生成した第1コンテンツ鍵を記録するコンテンツ鍵記録部1

206a1と、前記生成した第2コンテンツ鍵を記録するコンテンツ鍵記録部1206a2と、コンテンツ鍵記録部1206a1、206a2に記録された第1コンテンツ鍵、第2コンテンツ鍵へのアクセスを制御する制御部1203aと、前記第1コンテンツ鍵を用いて、前記受信したコンテンツを暗号化して、第1暗号化コンテンツを生成する暗号化部1208aと、前記第1暗号化コンテンツを記録する暗号化コンテンツ記録部1210aと、前記受信したコンテンツを、変換する変換部1207aと、前記第2コンテンツ鍵を用いて、前記変換したコンテンツを暗号化して第2暗号化コンテンツを生成する暗号化部1209aとを備える。

[0241] また、記録再生装置1102aは、さらに、前記第2暗号化コンテンツを記録する暗号化コンテンツ記録部1211aと、前記第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを、前記第1コンテンツ鍵、もしくは、前記第2コンテンツ鍵を用いて復号化する復号化部1221aと、復号した第1暗号化コンテンツ、もしくは、復号した第2暗号化コンテンツを再生する再生部1222aと、コピー制御情報記録部1204aに記録したコピー制御情報に基づいて、暗号化コンテンツ記録部1211aに記録した第2暗号化コンテンツを、記録再生装置1102aから可搬媒体1104aに移動することが認められているか否か判定する、もしくは、後述する可搬媒体1104aのコピー制御情報記録部1216aに記録したコピー制御情報に基づいて、可搬媒体1104aの暗号化コンテンツ記録部1218aに記録した第2暗号化コンテンツを、可搬媒体1104aから記録再生装置1102aに移動することが認められているか否か判定する判定部1212aと、記録再生装置1102aと可搬媒体1104aとの間で、相互に、相手が正当であるか否かを認証する認証部1223a、認証部1224aと、認証が成功した時に、記録再生装置1102aと可搬媒体1104aとの間で、やりとりされるコピー制御情報、並びに、第1コンテンツ鍵、もしくは、第2コンテンツ鍵を暗号化、復号化するための暗号化／復号化部1225a、226aと、コピー制御情報記録部1204aに記録したコピー制御情報と、コンテンツ鍵記録部1206a1に記録した第1コンテンツ鍵、もしくは、コンテンツ鍵記録部1206a2に記録した第2コンテンツ鍵と、並びに、暗号化コンテンツ記録部1211aに記録した第2暗号化コンテンツを可搬媒体1104aに書込む、もしくは、可搬媒体1104aから読み出す書込／読出部1213aとを備える。

[0242] 記録再生装置が備えるコピー制御情報記録部1204a、制御部1203a、並びに、コンテンツ鍵記録部1206a1、206a2は、外部からのデータの読み書きが不可能なセキュアな領域1214aに設けられる。この領域1214aは、具体的には、耐タンパハードウエア、耐タンパソフトウエア、あるいは、両者の組み合わせで構成する。暗号化コンテンツ記録部1210a、211aは、外部からの読み書きが可能な領域1215aに設けられる。この領域1215aは、例えば、HDD(Hard Disk Drive)により構成する。

[0243] 一方、可搬媒体1104aは、記録再生装置1102aと可搬媒体1104aとの間で、相互に、相手が正当であるか否かを認証する認証部1224aと、認証が成功した時に、記録再生装置1102aと可搬媒体1104aとの間で、やりとりされるコピー制御情報、並びに、第1コンテンツ鍵、もしくは、第2コンテンツ鍵を暗号化、復号化するための暗号化／復号化部1226aとを備える。

[0244] また、可搬媒体1104aは、さらに、前記第2暗号化コンテンツを記録する暗号化コンテンツ記録部1218aと、前記第1コンテンツ鍵、もしくは、第2コンテンツ鍵を記録するコンテンツ鍵記録部1217aと、前記コピー制御情報を記録するコピー制御情報記録部1216aを備える。可搬媒体1104aが備えるコピー制御情報記録部1216a、並びに、前記コンテンツ鍵記録部1217aは、外部から正当な装置以外読み書きできない領域1219aに設けられる。この領域1219aは、可搬媒体1104aの認証部1224aと、記録再生装置の認証部1223aとの間で、認証処理が正しく実行できた場合のみ、前記記録再生装置1102aからのデータの読み書き可能となる領域である。暗号化コンテンツ記録部1218aは、外部からの読み書きが可能な領域1220aに設けられる。

[0245] 次に、図37を用いて、受信したコンテンツを記録再生装置1102aに記録する場合の動作について説明する。

S501a:記録再生装置1102aの受信部1201aは、コンテンツとコピー制御情報を受信する。

S502a:判定部1202aは、「前記コピー制御情報が、受信したコンテンツを記録再生装置1102aに記録することが認められているか否か」を判定する。判定の結果、「記録は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結

果、「記録は認められる」と判定した場合は、以降の処理を実行する。

[0246] S503a：前記コピー制御情報を、必要に応じて更新してコピー制御情報記録部1204aに記録する。

S504a：鍵生成部1205aは、第1コンテンツ鍵、および、第2コンテンツ鍵を生成し、それぞれコンテンツ鍵記録部1206a1、206a2に記録する。

S505a：暗号化部1208aは、受信したコンテンツを、コンテンツ鍵記録部1206a1に記録している第1コンテンツ鍵で暗号化して第1暗号化コンテンツを生成する。

[0247] S506a：前記第1暗号化コンテンツを暗号化コンテンツ記録部1210aに記録する。

S507a：変換部1207aは、受信したコンテンツを、変換する。

S508a：暗号化部1209aは、前記変換したコンテンツを、コンテンツ鍵記録部1206a2に記録している第2コンテンツ鍵で暗号化して第2暗号化コンテンツを生成する。

[0248] S509a：前記第2暗号化コンテンツを暗号化コンテンツ記録部1211aに記録する。

ここで、コピー制御情報としては、実施例4の場合と同様に、例えば、コピーが禁止されていることを示す「Copy Never」や、コピーが1回だけ許されていることを示す「Copy One Generation」などが用いられる。この場合、判定部1202aは、コピー制御情報が「Copy Never」であれば、「記録は認められない」と判定し、コピー制御情報が「Copy One Generation」であれば、「記録は認められている」と判定する。後者の場合、コンテンツを記録再生装置に記録するのに伴い、コピー制御情報は、「Copy One Generation」から、これ以上コピー禁止を示す「No More Copy」へ更新してコピー制御情報記録部1204aに記録する。

[0249] 変換部1207aは、例えば、受信したコンテンツが、MPEG2形式の映像コンテンツである場合に、MPEG4形式の映像コンテンツに圧縮変換する。

次に、図38を用いて、記録再生装置1102aから、可搬媒体1104aへコンテンツを移動する場合の動作について説明する。

S401a：記録再生装置1102aの判定部1212aは、書込／読出部1213aを介して、コピー制御情報記録部1204aに記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部1211aに記録した第2暗号化コンテンツを可搬媒体1104aに移動することが認められているか否か」を判定する。判

定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

[0250] S402a：記録再生装置104aの認証部1223aは、可搬媒体1104aの認証部1224aとの間で相互認証を行い、相互認証が成功した時は、認証部1223a、224aはそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

S403a：書込／読出部1213aは、コピー制御情報記録部1204aに記録しているコピー制御情報、並びに、コンテンツ鍵記録部1206a2に記録している第2コンテンツ鍵を読み出す。

[0251] このとき、制御部1203aは、コンテンツ鍵記録部1206a1に記録している第1コンテンツ鍵および、コンテンツ鍵記録部1206a2に記録している第2コンテンツ鍵が、以降、アクセスできないように利用不可状態にする。

S404a：書込／読出部1213は、読み出したコピー制御情報、並びに、第2コンテンツ鍵を、暗号化／復号化部1225aにて、前記セッション鍵を用いて暗号化して可搬媒体1104aに送り、可搬媒体1104aは、受け取った暗号化したコピー制御情報、並びに、第2コンテンツ鍵を、暗号化／復号化部1226aにて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、第2コンテンツ鍵を可搬媒体1104aに記録する。

[0252] S405a：コピー制御情報記録部1204aに記録しているコピー制御情報、並びに、コンテンツ鍵記録部1206a2に記録している第2コンテンツ鍵を消去する。

S406a：書込／読出部1213aは、暗号化コンテンツ記録部1211aに記録している第2暗号化コンテンツを読出す。

S407a：読み出した第2暗号化コンテンツを可搬媒体1104aに記録する。

[0253] S408a：暗号化コンテンツ記録部1211aに記録している第2暗号化コンテンツを消去する。

図39、図40は、上記動作における記録再生装置1102a、並びに可搬媒体1104aにおける各データの記録状態を示した図である。図39(a)は、上記ステップS401aの開始時点、(b)は、上記ステップS403aの終了時点、(c)は、ステップS404aの終

了時点、(d)は、ステップS405aの終了時点、図40(e)は、ステップS407aの終了時点、(f)は、ステップS408aの終了時点である。

[0254] ここでステップS403aにおいて、制御部1203aは、コンテンツ鍵記録部1206a1に記録している第1コンテンツ鍵、及び、コンテンツ鍵記録部1206a2に記録している第2コンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。これにより、ステップS404aが終了し、ステップS405aが開始する前のタイミングで、電源断、もしくは、可搬媒体1104aを記録再生装置1102aから不正に引き抜く事などが行われたとしても、記録再生装置1102aと、可搬媒体1104aの両方において同時に、第1コンテンツ鍵と第2コンテンツ鍵が利用可能な状態で存在することを防止できる。また、図39(a)ー図40(f)のどのタイミングで電源断が起こっても、記録再生装置1102aと、可搬媒体1104aのいずれかにおいて第1コンテンツ鍵、及び、第2コンテンツ鍵は存在するため、移動元と移動先の両方で、第1コンテンツ鍵、及び、第2コンテンツ鍵が共に損なわれコンテンツが利用できなくなることはない。

[0255] ステップS402aにおける認証部1223a、224aで実行される相互認証、及び、セッション鍵共有方法としては、実施例4と同様に、例えば、チャレンジーレスポンス型の相互認証、セッション鍵共有方法を用いる。チャレンジーレスポンス型の相互認証、セッション鍵共有方法については、公知であるので説明は省略する。

次に、図41を用いて、可搬媒体1104aから、記録再生装置1102aへコンテンツを移動する場合の動作について説明する。

[0256] S601a:記録再生装置1102aの判定部1212aは、書込／読出部1213aを介して、可搬媒体1104aのコピー制御情報記録部1216aに記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、可搬媒体1104aの暗号化コンテンツ記録部1218aに記録した第2暗号化コンテンツを記録再生装置1102aに移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

[0257] S602a:記録再生装置104aの認証部1223aは、可搬媒体1104aの認証部1224aとの間で相互認証を行い、相互認証が成功した時は、認証部1223a、224aはそれ

ぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

S603a：書込／読出部1213aは、可搬媒体1104aのコピー制御情報記録部1216aに記録しているコピー制御情報、並びに、コンテンツ鍵記録部1217aに記録している第2コンテンツ鍵を読み出す。このとき、可搬媒体1104aの暗号化／復号化部1226aにて、コピー制御情報、並びに、第2コンテンツ鍵は、前記セッション鍵を用いて暗号化して、記録再生装置1102aに送り、記録再生装置1102aの暗号化／復号化部1225aは、受け取った暗号化したコピー制御情報、並びに、第2コンテンツ鍵を、前記セッション鍵を用いて復号して、書込／読出部1213aに送る。

[0258] S604a：書込／読出部1213aは、読み出したコピー制御情報、並びに、第2コンテンツ鍵を、記録再生装置1102aのコピー制御情報記録部1204a、並びに、コンテンツ鍵記録部1206a2にそれぞれ記録する。このとき、制御部1203aは、コンテンツ鍵記録部1206a2に記録した第2コンテンツ鍵はアクセスできないよう利用不可状態にする。

[0259] S605a：可搬媒体1104aのコピー制御情報記録部1216aに記録しているコピー制御情報、並びに、コンテンツ鍵記録部1217aに記録している第2コンテンツ鍵を消去する。

制御部1203aは、コンテンツ鍵記録部1206a2に記録したコンテンツ鍵、並びに、コンテンツ鍵記録部1206a1に記録した第1コンテンツ鍵を利用可能状態にする。

[0260] S606a：書込／読出部1213aは、可搬媒体1104aの暗号化コンテンツ記録部1218aに記録している第2暗号化コンテンツを読出す。

S607a：読み出した第2暗号化コンテンツを記録再生装置1102aの暗号化コンテンツ記録部1211aに記録する。

S608a：可搬媒体1104aの暗号化コンテンツ記録部1218aに記録している第2暗号化コンテンツを消去する。

[0261] 図42、図43は、上記動作における記録再生装置1102a、並びに可搬媒体1104aにおける各データの記録状態を示した図である。図42(a)は、上記ステップS601aの開始時点、(b)は、上記ステップS604aの終了時点、(c)は、ステップS605aの終

了時点、(d)は、ステップS607aの終了時点、図43(e)は、ステップS608aの終了時点である。

[0262] 次に、図44を用いて、記録再生装置1102aにおいて、記録した第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを再生する場合の動作について説明する。

S701a:復号化部1221aは、暗号化コンテンツ記録部1210a、もしくは、暗号化コンテンツ記録部1211aより、第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを読出す。

[0263] S702a:復号化部1221aは、コンテンツ鍵記録部1206a1より第1コンテンツ鍵を、もしくは、コンテンツ鍵記録部1206a2より第2コンテンツ鍵を読み出す。

このとき、制御部1203aは、コンテンツ鍵記録部1206a1に記録している第1コンテンツ鍵、及び、コンテンツ鍵記録部1206a2に記録している第2コンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。

[0264] S703a:復号化部1221aは、読み出した第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを、読み出した第1コンテンツ鍵、もしくは、第2コンテンツ鍵を用いて復号化する。

S704a:再生部1222aは、復号した第1暗号化コンテンツもしくは、第2暗号化コンテンツを再生する。

[0265] ここで、ステップS702aにおいて、制御部1203aにより、第1コンテンツ鍵、もしくは、第2コンテンツ鍵はアクセスできないよう利用不可状態にされるので、第1暗号化コンテンツの復号及び再生処理と、第2暗号化コンテンツの復号及び再生処理は、排他的にしか実行できない。

＜変形例＞

(1)上記実施例4、及び上記実施例5において、コンテンツ供給装置1101、1101aから記録再生装置1102、102aへのコンテンツの供給方法としては、地上波、あるいは、衛星などを介した放送、インターネットなどを介した通信、DVDなどの記録メディアを介した方法など、さまざまな方法が利用できる。

[0266] (2)上記実施例4、及び上記実施例5において、受信部1201、201aにて、受信したコンテンツや、コピー制御情報は、暗号化されていてもよい。この場合は、判定部1

202、202aで処理する前に、暗号化されたコンテンツやコピー制御情報は復号化するものとする。

(3)上記実施例4、及び上記実施例5では、受信したコンテンツから、1つの変換したコンテンツを作成し、暗号化して記録する構成を説明したが、この構成に限定されない。例えば、受信したコンテンツから、複数の異なる変換を施したコンテンツを作成し、暗号化して記録し、そのうちの一つないし複数を記録再生装置から可搬媒体に移動するように構成してもよい。また実施例4、及び実施例5では、受信したコンテンツ自身は変換しない構成としたが、受信したコンテンツ自身を、(第2暗号化コンテンツとは異なる形式で)変換したものであるとしてもよい。

[0267] (4)上記実施例4、及び上記実施例5では、記録再生装置1102、102aの鍵生成部1205、205aにて、コンテンツ鍵、第1コンテンツ鍵、第2コンテンツ鍵を生成し、コンテンツ鍵記録部1206、206a1、206a2に記録するものとしたが、この構成に限定されない。例えば、コンテンツ鍵は、外部で生成され、記録再生装置1102、102aに供給される構成としてもよい。

[0268] (5)上記実施例4、及び上記実施例5において、可搬媒体1104、104aとしては、例えば、SDメモリカードを用いることができる。この場合、認証部1223、224、223a、224a、及び、暗号化/復号化部1225、226、225a、226aは、CPRM SD規格により決められた方式に従って実行する。

(6)上記実施例4、及び上記実施例5では、第2暗号化コンテンツを、記録再生装置1102、102aから可搬媒体1104、104aに移動する場合について説明したが、第1暗号化コンテンツを記録再生装置1102、102aから可搬媒体1104、104aに移動するとしてもよい。

[0269] (7)上記実施例4、及び上記実施例5では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置から、別の記録再生装置へコンテンツを移動する構成であってもよい。

(8)このとき、例えば、記録再生装置1102、及び、記録再生装置1103の認証部、及び、暗号化/復号化部は、DTCP規格により決められた方式に従って実行する。

[0270] (9)上記実施例4、及び上記実施例5では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する際、記録再生装置、並びに可搬媒体に記録する各種データを消去する構成としたが、本発明はその構成に限定されるものではない。例えば、可搬媒体に記録する暗号化コンテンツは消去せずに、復号に必要なコンテンツ鍵だけを消去して、前記暗号化コンテンツを利用不可状態にする構成であってもよい。また、データの消去ではなく、データの一部を破壊して利用できない状態にする構成であってもよい。また、データの消去ではなく、データを不正にアクセスできない利用不可能状態にする構成であってもよい。

[0271] (10)上記実施例4、及び上記実施例5において、記録再生装置が、コンテンツの移動処理における状態遷移を記憶する記憶部を備える構成であってもよい。記録再生装置は、コンテンツの移動が正しく完了しなかった場合、前記記憶部に記憶する状態遷移に基づいて、コンテンツの移動処理を続けて行うか、コンテンツの移動処理を最初からやり直すかを判断する構成であってもよい。さらに、記録再生装置は、前記記憶部に記憶する状態遷移を利用者に通知する通知部を備える構成であってもよい。その場合、正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、あるいはコンテンツの移動処理を最初かやり直すかを決定する構成であってもよい。

[0272] (11)上記実施例4、及び上記実施例5において、記録再生装置、並びに可搬媒体が、コンテンツ鍵を移動後に消去する場合、コンテンツ鍵の受信側が、コンテンツ鍵の送信側に対して正しく受信できたことを通知して、送信側は前記通知に基づいて受信を確認した後に、コンテンツ鍵を消去する構成であってもよい。

(12)上記実施例4、及び上記実施例5において、コンテンツには当該コンテンツを一意に識別するための識別子が付与されており、可搬媒体に移動させたコンテンツを元の記録再生装置に戻す場合、前記記録再生装置は、自身が保持する暗号化コンテンツの識別子、並びに可搬媒体に記録する暗号化コンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。また、コンテンツには、コンテンツを一意に識別

する識別子の代わりに、移動元の記録再生装置を一意に識別する識別子が付与されている構成であってもよい。この場合、記録再生装置は、コンテンツに付与されている記録再生装置の識別子と、自身の識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。

[0273] (13)上記実施例4、及び上記実施例5において、複数のコンテンツに対する、第1暗号化コンテンツ、第2暗号化コンテンツをそれぞれ作成し、暗号化コンテンツ記録部1210、211、210a、211aに記録し、複数のコンテンツに対する、コピー制御情報、並びに、コンテンツ鍵(もしくは、第1コンテンツ鍵、第2コンテンツ鍵)を、それぞれコピー制御情報記録部1204、204a、コンテンツ鍵記録部1206、206a1、206a2に記録する構成としてもよい。この場合、コンテンツと、それに対応するコンテンツ鍵、並びに、コピー制御情報が分かるように、例えば、コンテンツ識別情報を、第1暗号化コンテンツ、及び、第2暗号化コンテンツを、暗号化コンテンツ記録部1210、211、210a、211aに記録するときに一緒に記録し、また、コピー制御情報、並びに、コンテンツ鍵(もしくは、第1コンテンツ鍵、第2コンテンツ鍵)を、それぞれ、コピー制御情報記録部1204、204a、並びに、コンテンツ鍵記録部1206、206a1、206a2に記録するときに、前記コンテンツ識別情報を一緒に記録する構成としてもよい。これにより、例えば、ある第2暗号化コンテンツを可搬媒体1104aに移動するとき、そのコンテンツ識別情報と同じコンテンツ識別情報を有するコピー制御情報、並びにコンテンツ鍵(もしくは、第1コンテンツ鍵、第2コンテンツ鍵)を、コピー制御情報記録部1204、204a、並びに、コンテンツ鍵記録部1206、206a1、206a2より見出すことが可能となる。

[0274] (14)上記実施例4、及び上記実施例5では、コンテンツは外部のコンテンツ供給装置により供給される構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置に挿入された記録媒体からコンテンツを読み出す構成であってもよい。

＜まとめ＞

(1)以上説明したように、本発明は、コンテンツを保持する第1の装置から第2の装置へコンテンツを移動する、もしくは、第2の装置から第1の装置へコンテンツを移動

することが可能な著作権保護システムであって、前記第1の装置は、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第2の装置は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記コンテンツ鍵を記録する鍵記録部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第2の装置のコンテンツ記録部に記録することを特徴とする著作権保護システムである。

[0275] (2)また、(1)の著作権保護システムにおいて、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録するとしても良い。

(3)また、(1)の著作権保護システムにおいて、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録するとしても良い。

[0276] (4)また、(1)の著作権保護システムにおいて、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を消去するとしても良い。

(5)また、(1)の著作権保護システムにおいて、前記第1の装置は、さらに認証部を備え、前記第2の装置は、さらに認証部を備え、前記第1の装置の認証部は、前記第

2の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録するとしても良い。

[0277] (6)また、(1)の著作権保護システムにおいて、前記第1の装置は、さらに、認証部、および、鍵暗号部を備え、前記第2の装置は、さらに認証部、および、鍵暗号部を備え、前記第1の装置の認証部は、前記第2の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第1の装置の認証部と、前記第2の装置の認証部は、それぞれ、セッション鍵を生成し、前記第1の装置の鍵暗号部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を前記セッション鍵で暗号化して第2の装置に送り、前記第2の装置の鍵暗号部は、受け取った暗号化されたコンテンツ鍵を前記セッション鍵で復号し、復号したコンテンツ鍵を前記第2の装置の鍵記録部に記録するとしても良い。

[0278] (7)また、(1)の著作権保護システムにおいて、前記第1の装置は、さらに、コピー制御情報を記録するコピー制御情報記録部と、前記コピー制御情報に基づいて、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動することが認められているか否かを判定する判定部を備えるとしても良い。

[0279] (8)また、(1)の著作権保護システムにおいて、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第2の装置から前記第1の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第2の装置の鍵記録部に記録しているコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第1の装置のコンテンツ記録部に記録するとしても良い。

[0280] (9)また、(8)の著作権保護システムにおいて、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部へ記録するコンテンツ鍵を利用不可能な状態にして、前記第2の装置の鍵記録部に記録しているコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第1の装置の鍵記録部へ記録するコンテンツ鍵を利用可能な状態にするとしても良い。

[0281] (10)また、(1)の著作権保護システムにおいて、コンテンツを、コンテンツ鍵で暗号化したものを第1の暗号化コンテンツとし、前記コンテンツを変換して得られた変換コンテンツを、前記コンテンツ鍵で暗号化したものを第2の暗号化コンテンツとするとしても良い。

(11)また、(1)の著作権保護システムにおいて、前記第1の装置が、記録再生装置であり、前記第2の装置が、前記記録再生装置により、データの読み書きが可能な可搬媒体であるとしても良い。

[0282] (12)また、本発明は、コンテンツを可搬媒体へ移動する、もしくは、可搬媒体からコンテンツを移動することが可能な記録再生装置であって、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記記録再生装置から前記可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記可搬媒体に記録することを特徴とする記録再生装置である。

[0283] (13)また、前記記録再生装置において、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録するとしても良い。

[0284] (14)また、本発明は、記録再生装置へコンテンツを移動する、もしくは、記録再生装置からコンテンツを移動することが可能な可搬媒体であって、前記可搬媒体は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツ

を復号するためのコンテンツ鍵を記録する鍵記録部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記記録再生装置から可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体の鍵記録部に記録し、前記記録再生装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記可搬媒体のコンテンツ記録部に記録することを特徴とする可搬媒体である。

[0285] (15)前記可搬媒体において、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録するとしても良い。

[0286] (16)また、本発明は、コンテンツを保持する第1の装置から第2の装置へコンテンツを移動する、もしくは、第2の装置から第1の装置へコンテンツを移動することが可能な著作権保護システムであって、前記第1の装置は、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツを復号するための第1のコンテンツ鍵、及び、前記第2の暗号化コンテンツを復号するための第2コンテンツ鍵を記録する鍵記録部と、前記第1のコンテンツ鍵、及び、第2のコンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第2の装置は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を記録する鍵記録部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第2の装置のコンテンツ記

録部に記録することを特徴とする著作権保護システムである。

[0287] （17）また、（16）の著作権保護システムにおいて、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、並びに、第2のコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録した第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を、前記第1の装置の鍵記録部から消去するとしても良い。

[0288] （18）また、（16）の著作権保護システムにおいて、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第2の装置から前記第1の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第1の装置のコンテンツ記録部に記録するとしても良い。

[0289] （19）また、（18）の著作権保護システムにおいて、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部へ記録する第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を利用不可能な状態にして、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を消去し、前記第1の装置の鍵記録部へ記録する第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を利用可能な状態にするとしても良い。

その他の変形例

[0290] （1）上記実施例では、記録再生装置から可搬媒体へコンテンツを移動する構成を有しているが、本発明は、記録再生装置から可搬媒体へのコンテンツの移動に限定されず、例えば、記録再生装置から、他の記録再生装置へコンテンツを移動する構成であってもよい。

（2）上記実施例では、記録再生装置から可搬媒体へコンテンツを移動するために、高画質コンテンツであるMPEG-2から、低画質コンテンツであるMPEG-4へ画像変

換する構成を有しているが、本発明において、画像変換は、MPEG-2からMPEG-4への変換に限定されず、非可逆変換であればよい。

[0291] (3)更には、画像変換を施したコンテンツを移動させるのではなく、画像変換を施さずに移動させる場合であっても、本発明に含まれる。具体的には、コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置であって、コンテンツが暗号化されて生成された第1暗号化コンテンツと、前記第1暗号化コンテンツを復号するための装置鍵と、前記装置鍵とは異なる媒体鍵とを記憶している記憶手段と、前記装置鍵を用いて前記暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、前記復号手段により生成された前記コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に書き込む書込手段と、第1記憶手段から前記装置鍵を消去する鍵消去手段とを備えるように構成してもよい。

[0292] (4)上記第2実施例において、記録再生装置20は、装置記録鍵K_{HDD}を装置固有鍵Kaで暗号化した後、可搬媒体14に移動する構成でもよい。上記第3実施例においても同様に、記録再生装置30は、コンテンツ鍵K_cを装置固有鍵Kaで暗号化した後、可搬媒体14に移動するように構成してもよい。

(5)上記実施例では、可搬媒体から記録再生装置へのコンテンツの移動処理では、移動元である可搬媒体が保持していた暗号化コンテンツ及び媒体記録鍵を共に消去する構成を有しているが、本発明は、この構成に限定されず、暗号化コンテンツ及び媒体記録鍵のいずれか一方を消去する構成であってもよい。

[0293] また、暗号化コンテンツ及び媒体記録鍵を消去せず、何れか一方のデータの一部を破壊して利用できない状態にする構成であってもよい。

(6)本発明は、記録再生装置がコンテンツの移動処理における状態遷移を記憶する記憶手段を備える構成であってもよい。具体的には、記録再生装置は、コンテンツの移動状態を保持する状態保持手段を備え、前記記録再生装置は、前記コンテンツの移動が正しく完了しなかった場合、前記状態保持手段が保持するコンテンツの移動状態を、利用者に通知するように構成してもよい。これにより、記録再生装置は、コンテンツ移動が正しく完了しなかった場合、前記状態保持手段が保持する状態に基

づいて、コンテンツの移動処理を続けるか、はじめからやり直すかなどを判断するように構成してもよい。

[0294] また、前記記録再生装置は、コンテンツの移動状態を利用者に通知する通知手段を備え、前記通知手段は、前記状態保持手段が保持するコンテンツの移動状態を、利用者に通知するように構成してもよい。更にこの場合は、コンテンツの移動が正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、はじめからやり直すかなどを決定するように構成してもよい。

[0295] (7)上記実施例において、記録再生装置及び可搬媒体が、鍵を移動した後、自機が保持する鍵を消去する場合、移動先の機器が鍵を正しく受信したか否かを確認後に、鍵を消去するように構成してもよい。この場合、移動先の機器から鍵を正しく受信した旨を移動元の機器に通知するように構成してもよい。

(8)上記実施例1において、記録再生装置10は、装置記録鍵K_{HDD}を装置固有鍵Kaで暗号化する構成を有しているが、本発明はこの構成に限定されない。例えば、装置固有鍵Kaではなく、複数の装置が共有する共有鍵でK_{HDD}を暗号化する構成でもよい。また、装置製造業者毎に割り当てられる製造業者固有鍵でK_{HDD}を暗号化する構成であってもよい。また、暗号化の処理毎に鍵を生成し、生成した鍵でK_{HDD}を暗号化する構成であってもよい。

[0296] (9)上記実施例では、記録再生装置は、外部のコンテンツ供給装置11から放送されるデジタル放送番組であるコンテンツを取得する構成を有しているが、本発明は、この構成に限定されないのは勿論である。例えば、記録再生装置は、当該記録再生装置に挿入された記録媒体に記録されているデジタルコンテンツを読み出す構成であってもよい。

(10)上記実施例の前提として、装置間において、DTCP規格で定められた認証手順に基づき相互認証を行い、認証に成功した場合に、コンテンツの移動を行う構成も本発明に含まれる。

[0297] (11)本発明において、記録再生装置が作成するタイトルリストのデータ構成は、図4に示したタイトルリスト125及び129に限定されない。例えば、タイトル情報として、コンテンツのサムネイル画像を用いる構成であってもよい。この場合、利用可能なコン

テンツについては、大きなサムネイル画像を表示し、利用不可能なコンテンツについては、小さなサムネイル画像を表示するなどして、利用可否に関する情報をユーザに提示する構成であってもよい。

[0298] （12）上記実施例では、記録再生装置が記録するコンテンツを暗号化するための鍵（装置鍵）と可搬媒体が記録するコンテンツを暗号化するための鍵（媒体鍵）とが、異なる鍵データである構成を有するが、本発明において上記の構成は必須ではなく、以下のような場合であっても本発明に含まれる。

コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置であって、コンテンツが暗号化されて生成された第1暗号化コンテンツとコンテンツ鍵とを記憶している記憶手段と、前記コンテンツ鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、前記復号手段により生成された前記コンテンツに非可逆変換を施し、変換コンテンツを生成する変換手段と、前記変換手段により生成された前記変換コンテンツを、前記コンテンツ鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、前記コンテンツ鍵及び前記第2暗号化コンテンツとを、前記可搬媒体に移動させる移動手段と、前記記憶手段から前記コンテンツ鍵を消去する鍵消去手段とを備えることを特徴とする。

[0299] ここで、前記鍵消去手段は、前記移動手段が、前記コンテンツ鍵を前記可搬媒体に書き込んだ後に、前記記憶手段から前記コンテンツ鍵を消去し、前記移動手段は、前記鍵消去手段が前記コンテンツ鍵を消去した後に、前記第2暗号化コンテンツを前記可搬媒体に移動させるように構成してもよい。

ここで、前記移動手段は、前記コンテンツ鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記鍵消去手段は、前記記憶手段から、前記コンテンツ鍵を消去した後の前記端末装置であって、当該端末装置は、更に、前記可搬媒体から前記コンテンツ鍵を読み出す読出手段を備え、前記読出手段により読み出された前記コンテンツ鍵を、前記記憶手段に格納するように構成してもよい。

[0300] また、本発明は、コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置で用いられるコンテンツ移動方法であって、前記端末装置は、コンテンツが暗号化されて生成された第1暗号化コンテンツとコンテンツ鍵とを記

憶しており、前記コンテンツ移動方法は、前記コンテンツ鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号ステップと、前記復号ステップにより生成された前記コンテンツに非可逆変換を施し、変換コンテンツを生成する変換ステップと、前記変換ステップにより生成された前記変換コンテンツを、前記コンテンツ鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化ステップと、前記コンテンツ鍵及び前記第2暗号化コンテンツとを、前記可搬媒体に移動させる移動ステップと、前記端末装置から前記コンテンツ鍵を消去する鍵消去ステップとを含むことを特徴とする。

[0301] ここで、前記鍵消去ステップは、前記移動ステップが、前記コンテンツ鍵を前記可搬媒体に書き込んだ後に、前記端末装置から前記コンテンツ鍵を消去し、前記移動ステップは、前記鍵消去ステップが前記コンテンツ鍵を消去した後に、前記第2暗号化コンテンツを前記可搬媒体に移動させてもよい。

また、本発明は、コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置で用いられるコンテンツ移動プログラムであって、前記端末装置は、コンテンツが暗号化されて生成された第1暗号化コンテンツとコンテンツ鍵とを記憶しており、前記コンテンツ移動プログラムは、前記コンテンツ鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号ステップと、前記復号ステップにより生成された前記コンテンツに非可逆変換を施し、変換コンテンツを生成する変換ステップと、前記変換ステップにより生成された前記変換コンテンツを、前記コンテンツ鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化ステップと、前記コンテンツ鍵及び前記第2暗号化コンテンツとを、前記可搬媒体に移動させる移動ステップと、前記端末装置から前記コンテンツ鍵を消去する鍵消去ステップとを含むことを特徴とする。

[0302] ここで、前記鍵消去ステップは、前記移動ステップが、前記コンテンツ鍵を前記可搬媒体に書き込んだ後に、前記端末装置から前記コンテンツ鍵を消去し、前記移動ステップは、前記鍵消去ステップが前記コンテンツ鍵を消去した後に、前記第2暗号化コンテンツを前記可搬媒体に移動させてもよい。

(13)本発明において、記録再生装置からコンテンツをムーブされる可搬媒体は、S

Dメモリカードなどのカード型メモリに限定されないのは勿論であり、読み出し及び書き込み可能なDVDなどであってもよい。

[0303] (14)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0304] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0305] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(15)上記実施例及び上記変形例をそれぞれ組み合わせる構成も本発明に含まれる。

産業上の利用可能性

[0306] 本発明は、コンテンツをユーザに配信する産業、コンテンツを記録再生する装置を製造する製造業、コンテンツを記録再生する装置を販売する販売業において、画像変換したコンテンツを他の装置へムーブしても、元のコンテンツを復元可能であることから、ユーザの利便性を損なわず、コンテンツの著作権を保護する仕組みとして利用することができる。

請求の範囲

[1] コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置であって、

コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶している記憶手段と、

前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、

前記復号手段により復号されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換手段と、

前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、

前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶手段から読み出し、前記可搬媒体に書き込む書込手段と、

前記記憶手段から前記装置鍵を消去する鍵消去手段とを備える

ことを特徴とする端末装置。

[2] 前記鍵消去手段は、前記書込手段が、前記装置鍵を前記可搬媒体に書き込んだ後に、前記記憶手段から前記装置鍵を消去し、

前記書込手段は、前記鍵消去手段が前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させる

ことを特徴とする請求項1に記載の端末装置。

[3] 前記記憶手段は、前記装置鍵を暗号化するための鍵情報を記憶しており、

前記暗号化手段は、前記鍵情報を用いて前記装置鍵を暗号化し、暗号化装置鍵を生成し、

前記書込手段は、前記装置鍵に替えて前記暗号化手段により生成された前記暗号化装置鍵を前記可搬媒体に書き込む

ことを特徴とする請求項2に記載の端末装置。

[4] 前記書込手段は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記暗号化装置鍵を前記可搬媒体に書き込み、前記鍵消去手段は、前

記記憶手段から前記装置鍵を消去した後の前記端末装置であって、

当該端末装置は、

前記暗号化装置鍵を前記可搬媒体から読み出す読出手段を備え、

前記復号手段は、前記鍵情報を用いて前記暗号化装置鍵を復号し、前記装置鍵を生成し、生成した前記装置鍵を前記記憶手段に格納する

ことを特徴とする請求項3に記載の端末装置。

[5] 前記端末装置は、更に、

前記変換手段により生成された前記変換コンテンツに、前記装置鍵を埋め込み、鍵埋込コンテンツを生成する埋込手段を備え、

前記暗号化手段は、前記埋込手段により生成された前記鍵埋込コンテンツを、前記媒体鍵を用いて暗号化することにより前記第2暗号化コンテンツを生成し、

前記鍵消去手段は、前記埋込手段が、前記装置鍵を前記変換コンテンツに埋め込んだ後に、前記記憶手段から前記装置鍵を消去し、

前記書込手段は、前記鍵消去手段が前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させる

ことを特徴とする請求項1に記載の端末装置。

[6] 前記書込手段は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記鍵消去手段は、前記記憶手段から前記装置鍵を消去した後の前記端末装置であって、

当該端末装置は、更に、

前記鍵埋込コンテンツから前記装置鍵を抽出し、抽出した前記装置鍵を前記記憶手段に格納する抽出手段を備え、

前記読出手段は、前記可搬媒体から前記第2暗号化コンテンツ及び前記媒体鍵を読み出し、

前記復号手段は、前記媒体鍵を用いて前記第2暗号化コンテンツを復号し、前記鍵埋込コンテンツを生成し、生成した前記鍵埋込コンテンツを前記抽出手段に出力する

ことを特徴とする請求項5に記載の端末装置。

[7] 前記書込手段は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記装置鍵を前記可搬媒体に書き込み、前記鍵消去手段は、前記記憶手段から、前記装置鍵を消去した後の前記端末装置であって、

当該端末装置は、更に、

前記可搬媒体から前記装置鍵を読み出す読出手段を備え、

前記読出手段により読み出された前記装置鍵を、前記記憶手段に格納する

ことを特徴とする請求項1に記載の端末装置。

[8] 前記端末装置は、更に、

前記コンテンツを再生する再生手段を備え、

前記復号手段は、前記記憶手段から、前記第1暗号化コンテンツと前記装置鍵とを読み出し、読み出した前記装置鍵を用いて前記第1暗号化コンテンツを復号して前記コンテンツを生成し、生成した前記コンテンツを前記再生手段へ出力する

ことを特徴とする請求項7に記載の端末装置。

[9] コンテンツの著作権を保護しつつ、コンテンツの利用権を端末装置から可搬媒体へ移動させるコンテンツ保護システムであって、

前記端末装置は、

コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶している第1記憶手段と、

前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、

前記復号手段により生成されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換手段と、

前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、

前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記記憶手段から前記装置鍵を読み出し、前記可搬媒体に書き込む書込手段と、

前記第1記憶手段から前記装置鍵を消去する鍵消去手段とを備え、

前記可搬媒体は、

前記端末装置から受け取る前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを記憶する第2記憶手段を備え、

前記鍵消去手段は、前記書込手段が、前記装置鍵を前記第2記憶手段に書き込んだ後に、前記記憶手段から前記装置鍵を消去し、

前記書込手段は、前記鍵消去手段が前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させる

ことを特徴とするコンテンツ保護システム。

[10] 前記書込手段は、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させ、前記装置鍵を前記可搬媒体に書き込み、前記鍵消去手段は、前記記憶手段から、前記装置鍵を消去した後の前記コンテンツ保護システムであって、

前記端末装置は、更に、

前記第2記憶手段から前記装置鍵を読み出す読出手段を備え、

前記読出手段により読み出された前記装置鍵を、前記第1記憶手段に格納し、

前記可搬媒体は、更に、

前記第2記憶手段に格納されている前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去する消去手段を備え、

前記読出手段は、前記消去手段が前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去した後、前記装置鍵を読み出す

ことを特徴とする請求項9に記載のコンテンツ保護システム。

[11] 前記第1記憶手段は、前記装置鍵を暗号化するための鍵情報を記憶しており、

前記暗号化手段は、前記鍵情報を用いて前記装置鍵を暗号化し、暗号化装置鍵を生成し、

前記書込手段は、前記装置鍵に替えて前記暗号化手段により生成された前記暗号化装置鍵を前記第2記憶手段に書き込み、前記暗号化装置鍵を書き込んだ後に、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記憶手段に移動させ、

前記第2記憶手段は、前記装置鍵に替えて、前記暗号化装置鍵を記憶する

ことを特徴とする請求項9に記載のコンテンツ保護システム。

[12] 前記書込手段は、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記憶手段

に移動させ、前記暗号化装置鍵を前記第2記憶手段に書き込み、前記鍵消去手段は、前記第1記憶手段から前記装置鍵を消去した後の前記コンテンツ保護システムであって、

前記端末装置は、更に、

前記暗号化装置鍵を前記第2記憶手段から読み出す読出手段を備え、

前記復号手段は、前記鍵情報を用いて前記暗号化装置鍵を復号して前記装置鍵を生成し、生成した前記装置鍵を前記第1記憶手段に格納し、

前記可搬媒体は、更に、

前記第2記憶手段に格納されている前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去する消去手段を備え、

前記読出手段は、前記消去手段が前記第2暗号化コンテンツ及び前記媒体鍵の内少なくとも一方を消去した後、前記暗号化装置鍵を読み出す

ことを特徴とする請求項11に記載のコンテンツ保護システム。

[13] 前記端末装置は、更に、

前記変換手段により生成された前記変換コンテンツに、前記装置鍵を埋め込み、鍵埋込コンテンツを生成する埋込手段を備え、

前記暗号化手段は、前記埋込手段により生成された前記鍵埋込コンテンツを、前記媒体鍵を用いて暗号化することにより前記第2暗号化コンテンツを生成し、

前記鍵消去手段は、前記埋込手段が、前記装置鍵を前記変換コンテンツに埋め込んだ後に、前記第1記憶手段から前記装置鍵を消去し、

前記書込手段は、前記鍵消去手段が前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記憶手段に書き込む

ことを特徴とする請求項9に記載のコンテンツ保護システム。

[14] 前記書込手段は、前記媒体鍵及び前記第2暗号化コンテンツを前記第2記憶手段に移動させ、前記鍵消去手段は、前記第1記憶手段から前記装置鍵を消去した後の前記コンテンツ保護システムであって、

前記端末装置は、更に、

前記鍵埋込コンテンツから前記装置鍵を抽出し、抽出した前記装置鍵を前記第1

記憶手段に格納する抽出手段を備え、

前記読出手段は、前記第2記憶手段から前記第2暗号化コンテンツ及び前記媒体鍵を読み出し、

前記復号手段は、前記媒体鍵を用いて前記第2暗号化コンテンツを復号し、前記鍵埋込コンテンツを生成し、生成した前記鍵埋込コンテンツを前記抽出手段に出力し、

前記可搬媒体は、

前記端末装置により、前記第2暗号化コンテンツ及び前記媒体鍵が読み出されると、前記第2記憶手段から、前記第2暗号化コンテンツ及び前記媒体鍵を消去する

ことを特徴とする請求項13に記載のコンテンツ保護システム。

[15] 前記コンテンツ保護システムは、更に、携帯情報端末を含み、

前記携帯情報端末は、前記第2記憶手段に、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツが記憶された前記可搬媒体から、前記第2暗号化コンテンツと前記媒体鍵とを読み出し、読み出した前記第2暗号化コンテンツを、前記媒体鍵を用いて復号して、前記変換コンテンツを生成し、生成した前記変換コンテンツを再生する

ことを特徴とする請求項9に記載のコンテンツ保護システム。

[16] 前記コンテンツ保護システムは、更に、

前記端末装置と接続された他の端末装置を備え、

前記他の端末装置は、

前記第2記憶手段に、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツが記憶された前記可搬媒体から、前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを読み出す読出手段と、

前記読出手段が読み出した前記媒体鍵及び前記第2暗号化コンテンツの内少なくとも一方を消去する消去手段と、

前記消去手段により、前記媒体鍵及び前記第2暗号化コンテンツの内少なくとも一方が消去されると、前記端末装置から前記第1暗号化コンテンツを取得する取得手段とを備え、

前記可搬媒体は、

前記他の端末装置へ前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを移動させ、

前記端末装置は、更に、

前記他の端末装置へ、前記第1暗号化コンテンツを送信する送信手段と、

前記第1記憶手段から前記第1暗号化コンテンツを消去するコンテンツ消去手段とを備える

ことを特徴とする請求項9に記載のコンテンツ保護システム。

[17] コンテンツの著作権を保護しつつ、端末装置から前記コンテンツの利用権の移動を受け付ける可搬媒体であって、

前記記録装置は、

コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶している記憶手段と、

前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、

前記復号手段により復号されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換手段と、

前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、

前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶手段から読み出し、前記可搬媒体に書き込む書込手段と、

前記記憶手段から前記装置鍵を消去する鍵消去手段とを備え、

前記可搬媒体は、

前記媒体鍵、前記第2暗号化コンテンツ及び前記装置鍵を記憶する記憶手段を備える

ことを特徴とする可搬媒体。

[18] コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置で用いられるコンテンツ移動方法であって、

前記端末装置は、コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶しており、

前記コンテンツ移動方法は、

前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号ステップと、

前記復号手段により復号されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換ステップと、

前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化ステップと、

前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶手段から読み出し、前記可搬媒体に書き込む書込ステップと、

前記端末装置から前記装置鍵を消去する鍵消去ステップと含む

ことを特徴とするコンテンツ移動方法。

[19] 前記鍵消去ステップは、前記書込ステップが、前記装置鍵を前記可搬媒体に書き込んだ後に、前記端末装置から前記装置鍵を消去し、

前記書込ステップは、前記鍵消去ステップが前記端末装置から前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させる

ことを特徴とする請求項18に記載のコンテンツ移動方法。

[20] コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置で用いられるコンテンツ移動プログラムであって、

前記端末装置は、コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶しており、

前記コンテンツ移動プログラムは、

前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号ステップと、

前記復号手段により復号されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換ステップと、

前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号

化し、第2暗号化コンテンツを生成する暗号化ステップと、

前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶手段から読み出し、前記可搬媒体に書き込む書込ステップと、

前記端末装置から前記装置鍵を消去する鍵消去ステップと含む

ことを特徴とするコンテンツ移動プログラム。

[21] 前記鍵消去ステップは、前記書込ステップが、前記装置鍵を前記可搬媒体に書き込んだ後に、前記端末装置から前記装置鍵を消去し、

前記書込ステップは、前記鍵消去ステップが前記端末装置から前記装置鍵を消去した後に、前記媒体鍵及び前記第2暗号化コンテンツを前記可搬媒体に移動させる

ことを特徴とする請求項20に記載のコンテンツ移動プログラム。

補正書の請求の範囲

[2005年4月29日（29．04．05）国際事務局受理：出願当初の
請求の範囲17は補正された；他の請求の範囲は変更なし。（1頁）]

前記可搬媒体は、

前記他の端末装置へ前記装置鍵、前記媒体鍵及び前記第2暗号化コンテンツを移動させ、

前記端末装置は、更に、

前記他の端末装置へ、前記第1暗号化コンテンツを送信する送信手段と、

前記第1記憶手段から前記第1暗号化コンテンツを消去するコンテンツ消去手段とを備える

ことを特徴とする請求項9に記載のコンテンツ保護システム。

[17] （補正後）コンテンツの著作権を保護しつつ、端末装置から前記コンテンツの利用権の移動を受け付ける可搬媒体であって、

前記端末装置は、

コンテンツが暗号化されて生成された第1暗号化コンテンツと装置鍵と媒体鍵とを記憶している記憶手段と、

前記装置鍵を用いて前記第1暗号化コンテンツを復号し、前記コンテンツを生成する復号手段と、

前記復号手段により復号されたコンテンツに非可逆変換を施し、変換コンテンツを生成する変換手段と、

前記変換手段により生成された前記変換コンテンツを、前記媒体鍵を用いて暗号化し、第2暗号化コンテンツを生成する暗号化手段と、

前記媒体鍵及び前記第2暗号化コンテンツを、前記可搬媒体に移動させ、前記装置鍵を前記記憶手段から読み出し、前記可搬媒体に書き込む書込手段と、

前記記憶手段から前記装置鍵を消去する鍵消去手段とを備え、

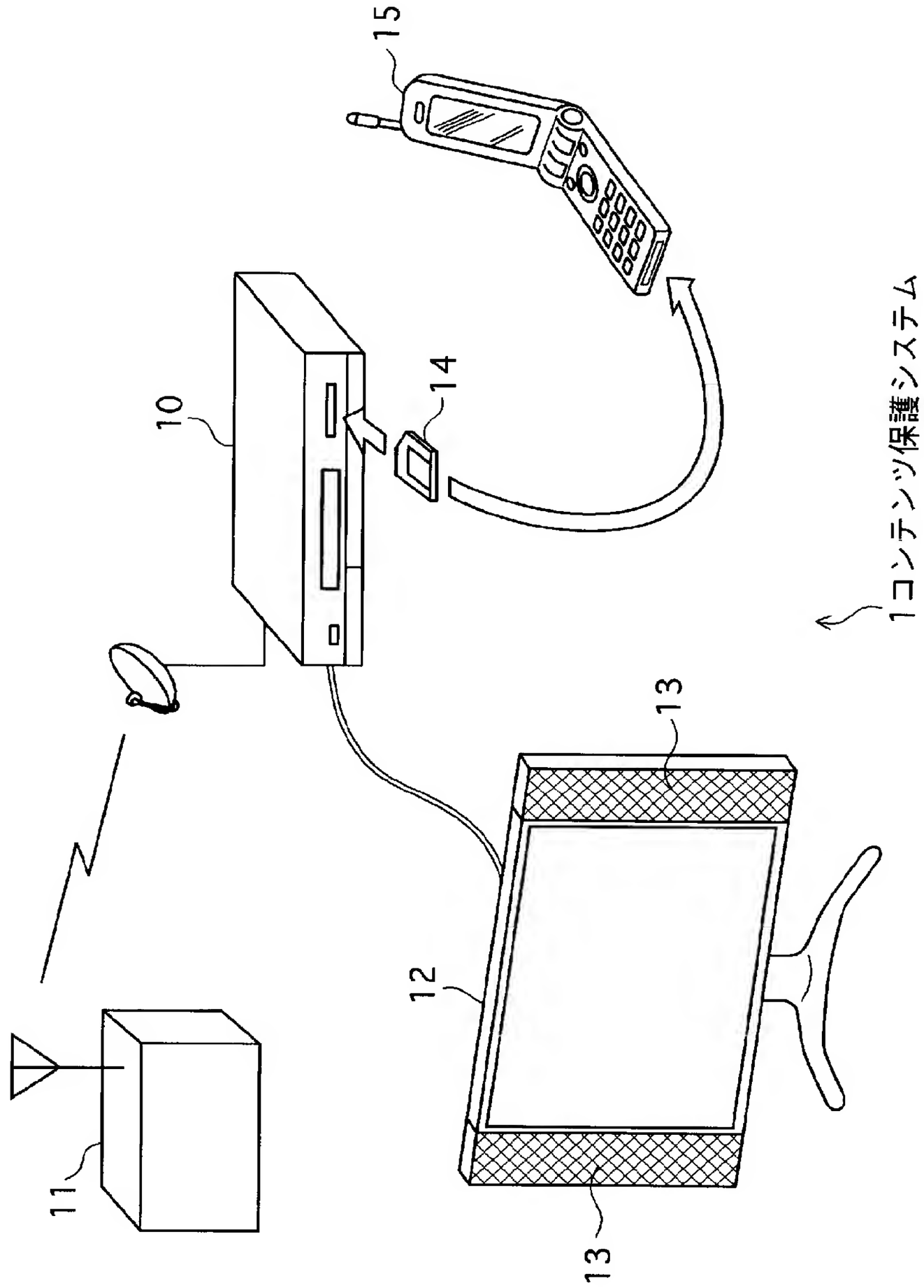
前記可搬媒体は、

前記媒体鍵、前記第2暗号化コンテンツ及び前記装置鍵を記憶する記憶手段を備える

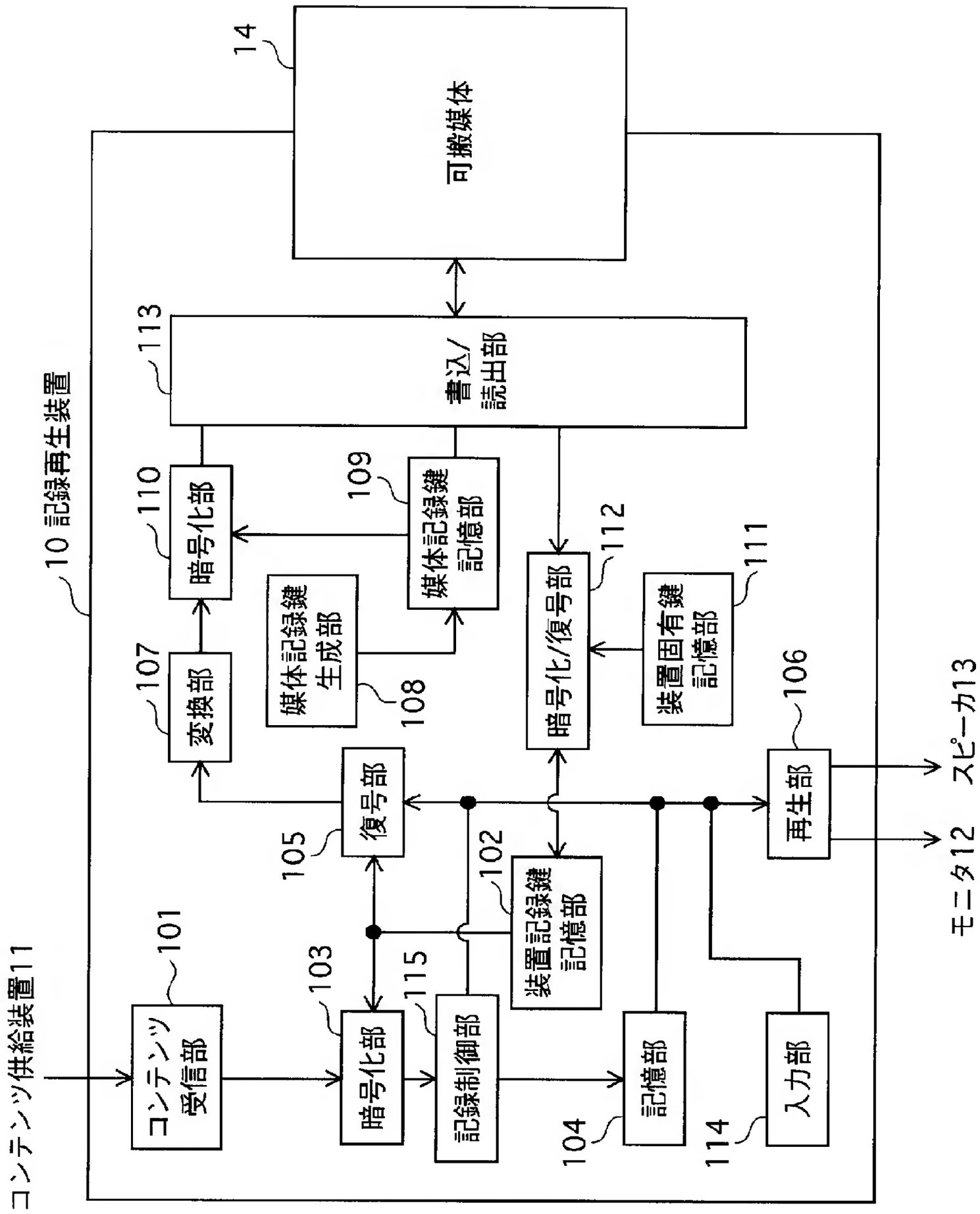
ことを特徴とする可搬媒体。

[18] コンテンツの著作権を保護しつつ、コンテンツの利用権を可搬媒体へ移動させる端末装置で用いられるコンテンツ移動方法であって、

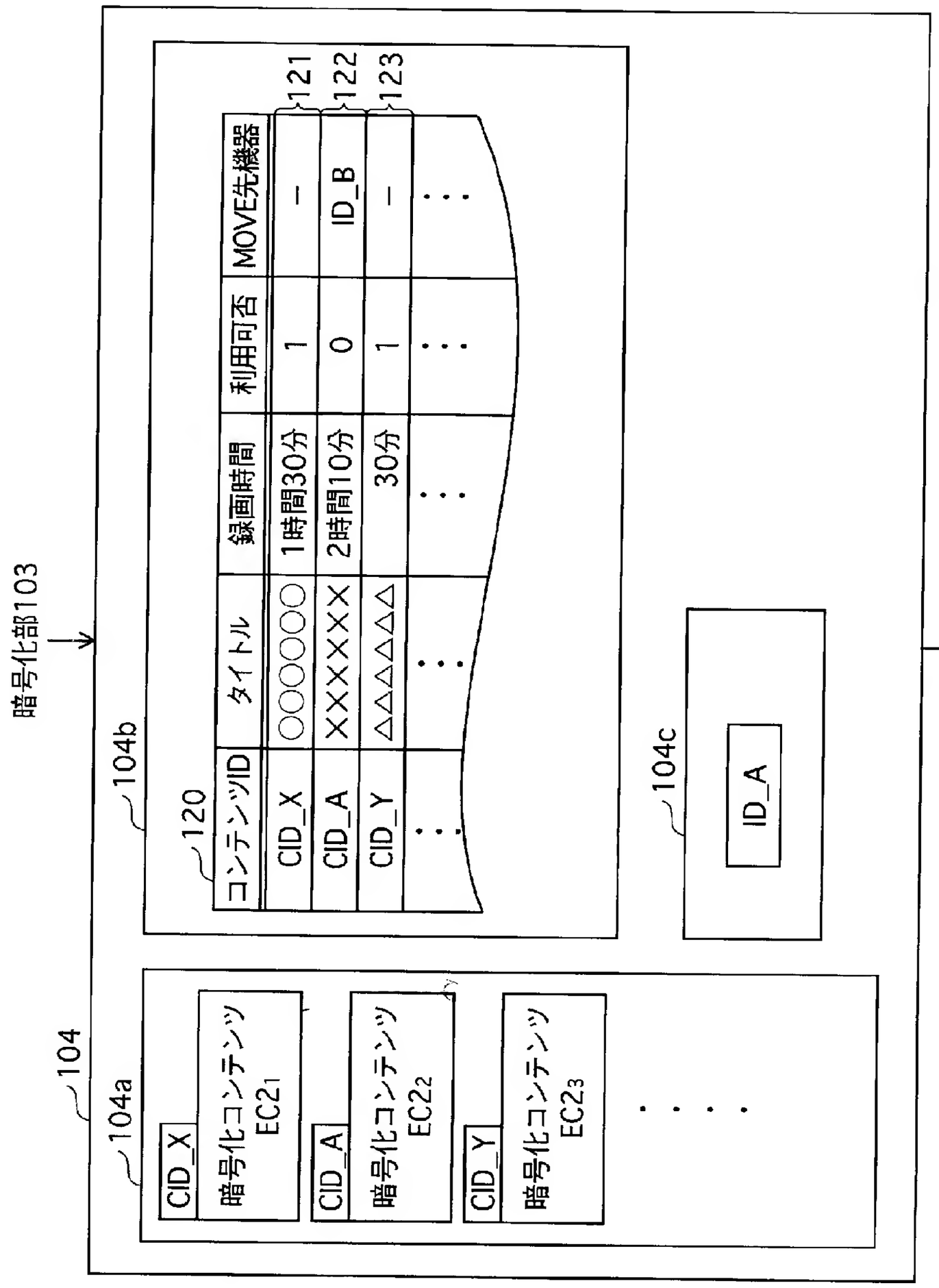
[図1]



[図2]


14
可搬媒体
113
書込/
読出部
10 記録再生装置
110
暗号化部
109
媒体記録鍵
記憶部
107
変換部
媒体記録鍵
生成部
108
暗号化/復号部
112
装置固有鍵
記憶部
111
106
再生部
105
復号部
102
装置記録鍵
記憶部
101
103
115
コンテンツ
受信部
暗号化部
記録制御部
104
記憶部
114
入力部
コンテンツ供給装置11
モニタ12
スピーカ13

[図3]


暗号化部103
104
104a
CID_X
暗号化コンテンツ EC2₁
CID_A
暗号化コンテンツ EC2₂
CID_Y
暗号化コンテンツ EC2₃
104b
120
コンテンツID
タイトル
録画時間
利用可否
MOVE先機器
121
122
123
CID_X
○○○○○○
1時間30分
1
—
CID_A
××××××
2時間10分
0
ID_B
CID_Y
△△△△△△
30分
1
—
104c
ID_A
復号部105

[図4]

(a)

125

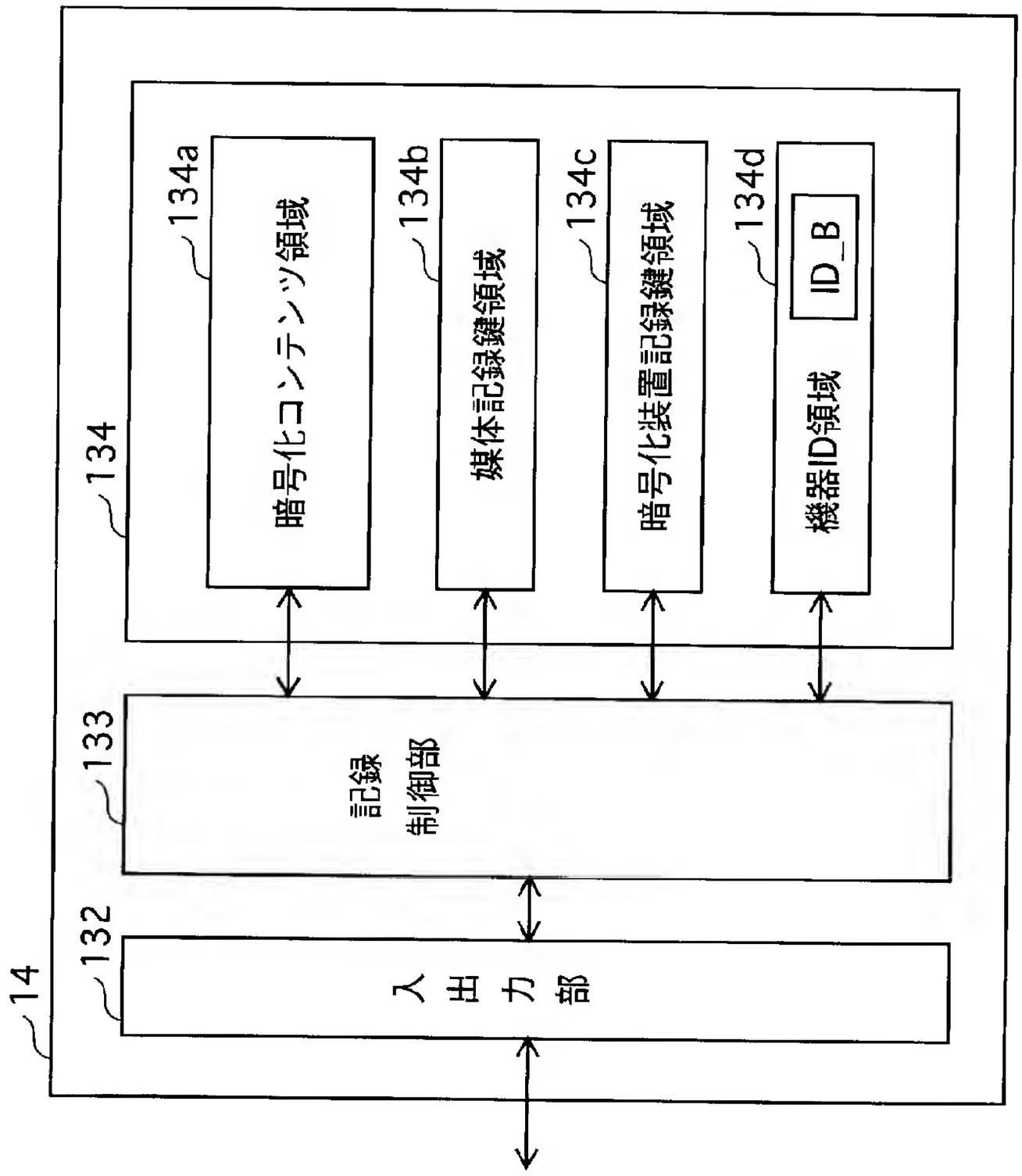
タイトル	記録時間	利用可否	
○○○○○○	1時間30分	○	126
××××××	2時間10分	×	127
△△△△△△	30分	○	128
⋮	⋮	⋮	

(b)

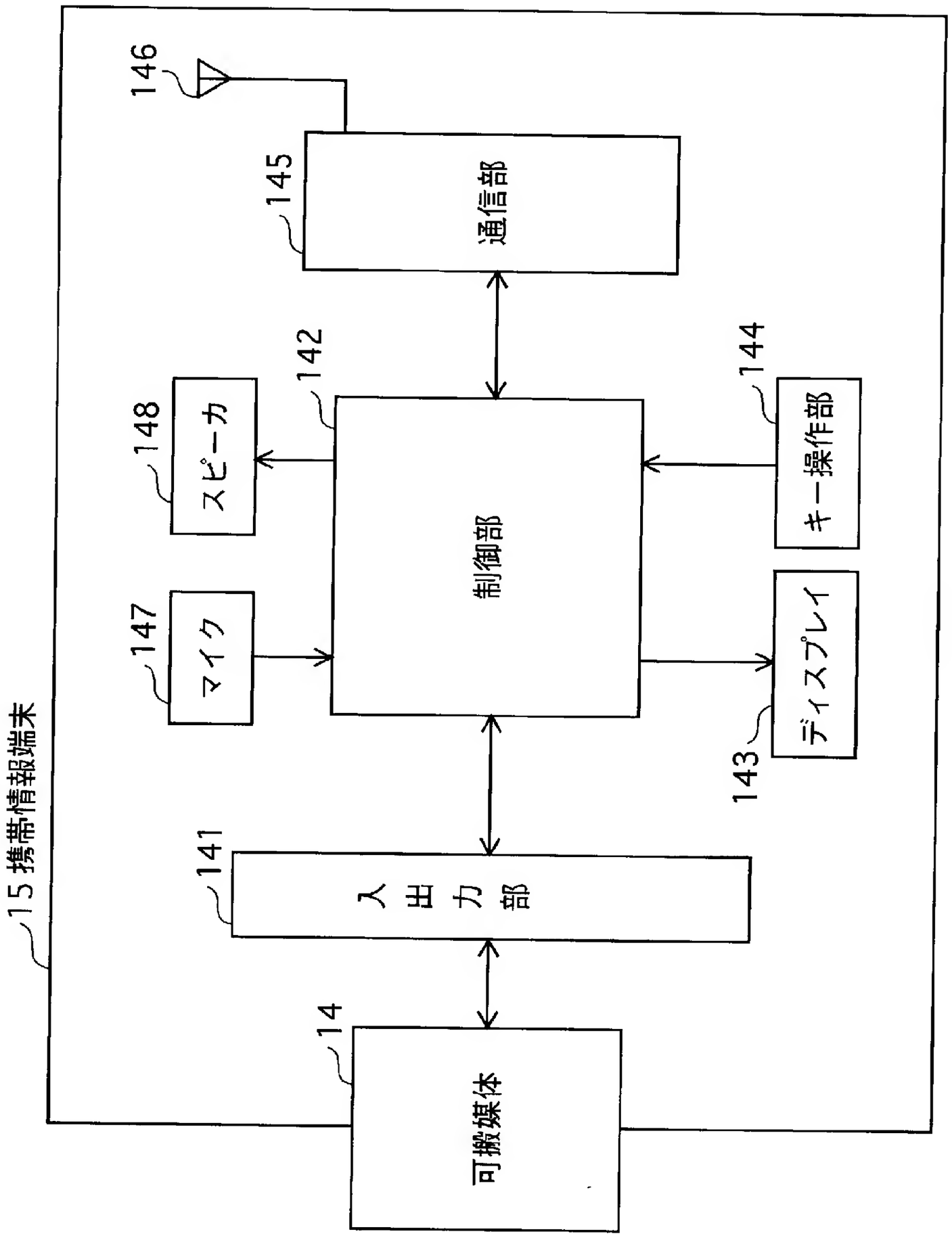
129

タイトル	記録時間	
○○○○○○	1時間30分	130
△△△△△△	30分	131
	⋮	

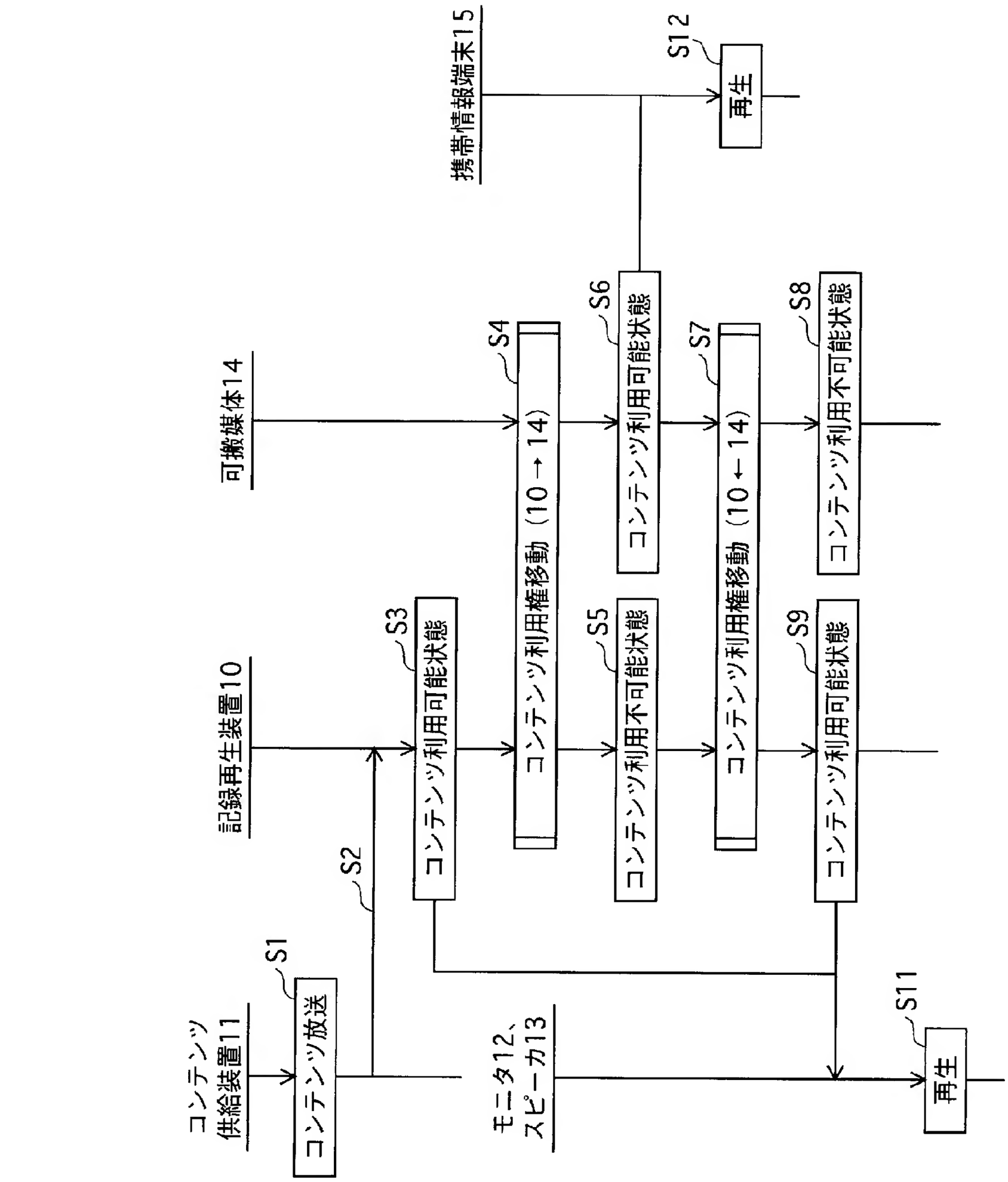
[図5]


14
132
入出力部
133
記録制御部
134
134a
暗号化コンテンツ領域
134b
媒体記録鍵領域
134c
暗号化装置記録鍵領域
134d
機器ID領域
ID_B

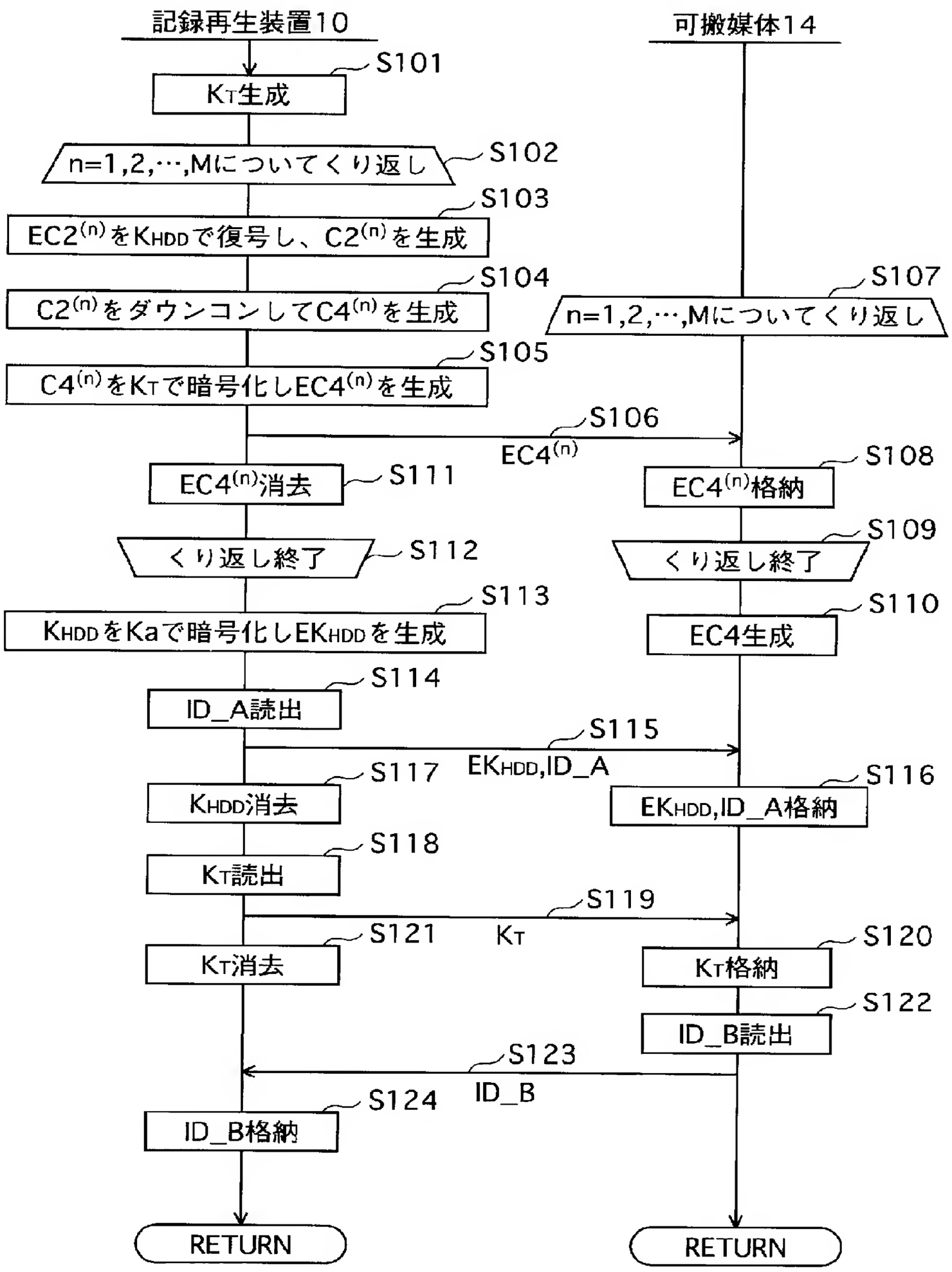
[図6]


15 携帯情報端末
146
145
通信部
141
入出力部
14
可搬媒体
142
制御部
148
スピーカ
147
マイク
144
キー操作部
143
ディスプレイ

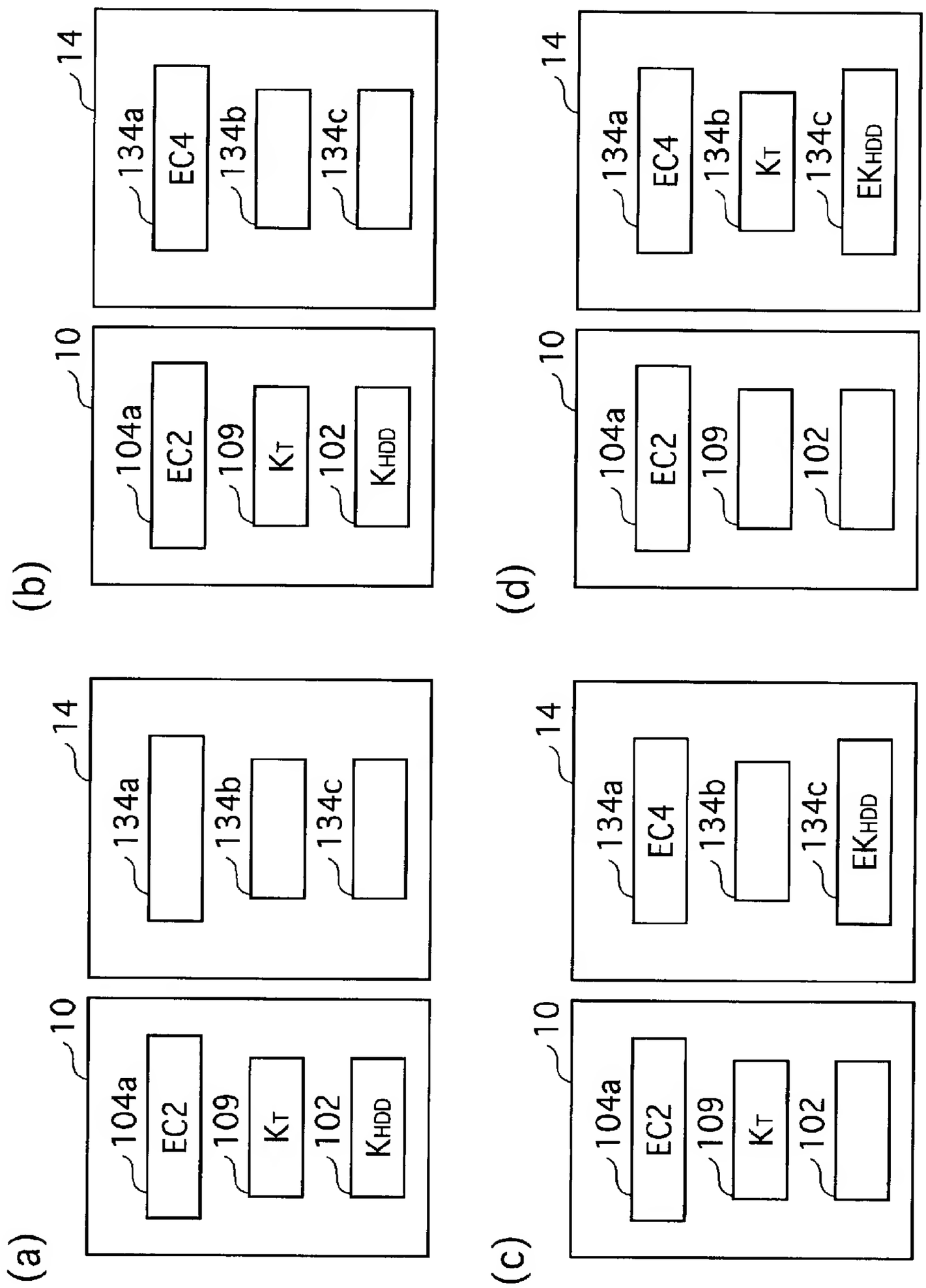
[図7]


携帯情報端末15
S12
再生
可搬媒体14
S4
コンテンツ利用権移動（10→14）
S6
コンテンツ利用可能状態
S7
コンテンツ利用権移動（10←14）
S8
コンテンツ利用不可能状態
記録再生装置10
S3
コンテンツ利用可能状態
S5
コンテンツ利用不可能状態
S9
コンテンツ利用可能状態
S2
コンテンツ
供給装置11
S1
コンテンツ放送
モニタ12、
スピーカ13
S11
再生

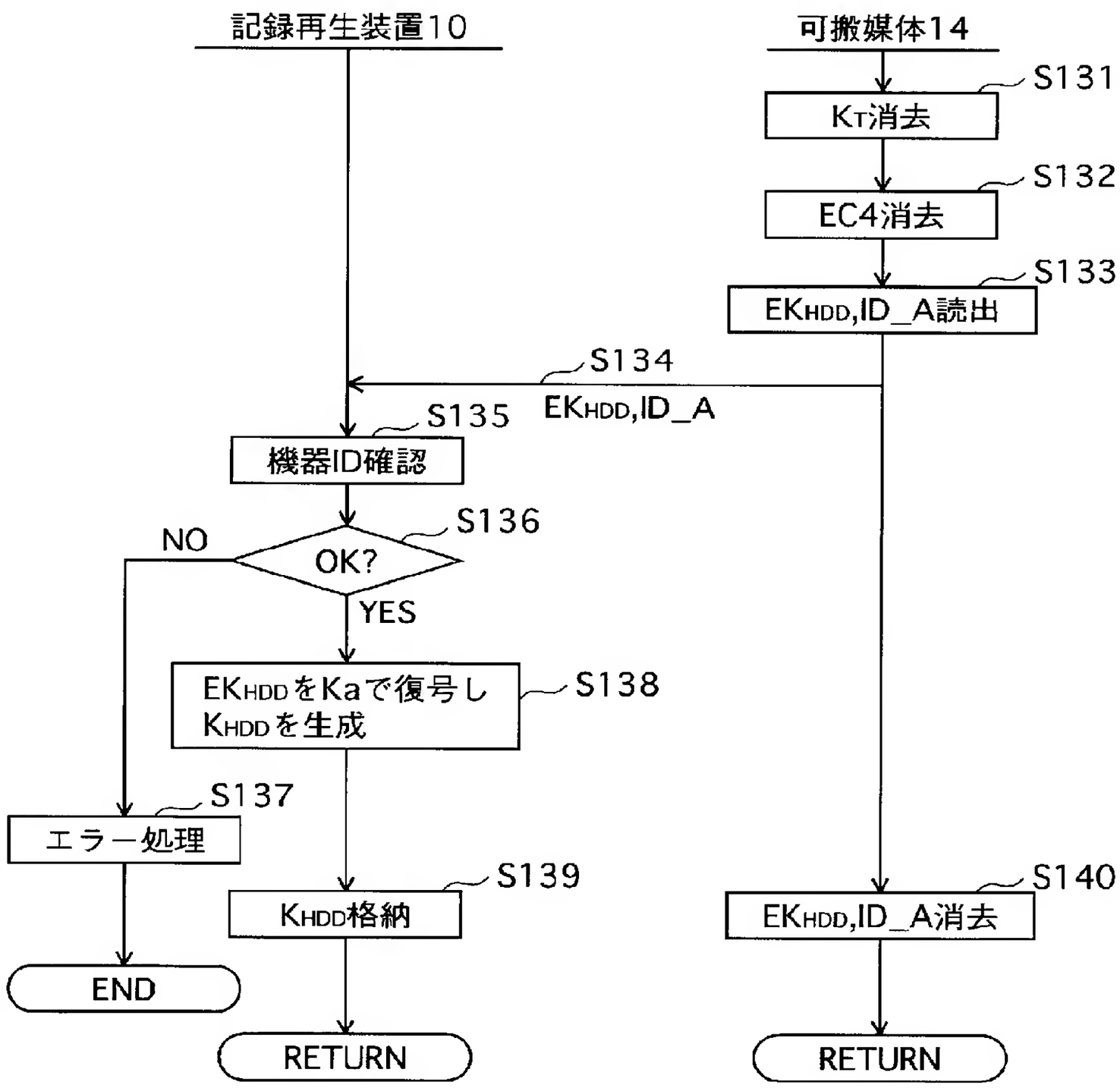
[図8]


記録再生装置10
可搬媒体14
S101
KT生成
S102
n=1,2,…,Mについてくり返し
S103
EC2(n)をKHDDで復号し、C2(n)を生成
S104
C2(n)をダウンコンしてC4(n)を生成
S105
C4(n)をKTで暗号化しEC4(n)を生成
S107
n=1,2,…,Mについてくり返し
S106
EC4(n)
S111
EC4(n)消去
S108
EC4(n)格納
S112
くり返し終了
S109
くり返し終了
S113
KHDDをKaで暗号化しEKHDDを生成
S110
EC4生成
S114
ID_A読出
S115
EKHDD,ID_A
S117
KHDD消去
S116
EKHDD,ID_A格納
S118
KT読出
S119
KT
S121
KT消去
S120
KT格納
S122
ID_B読出
S123
ID_B
S124
ID_B格納
RETURN
RETURN

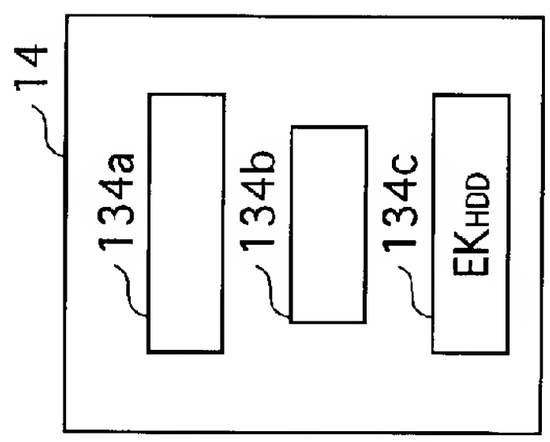
[図9]

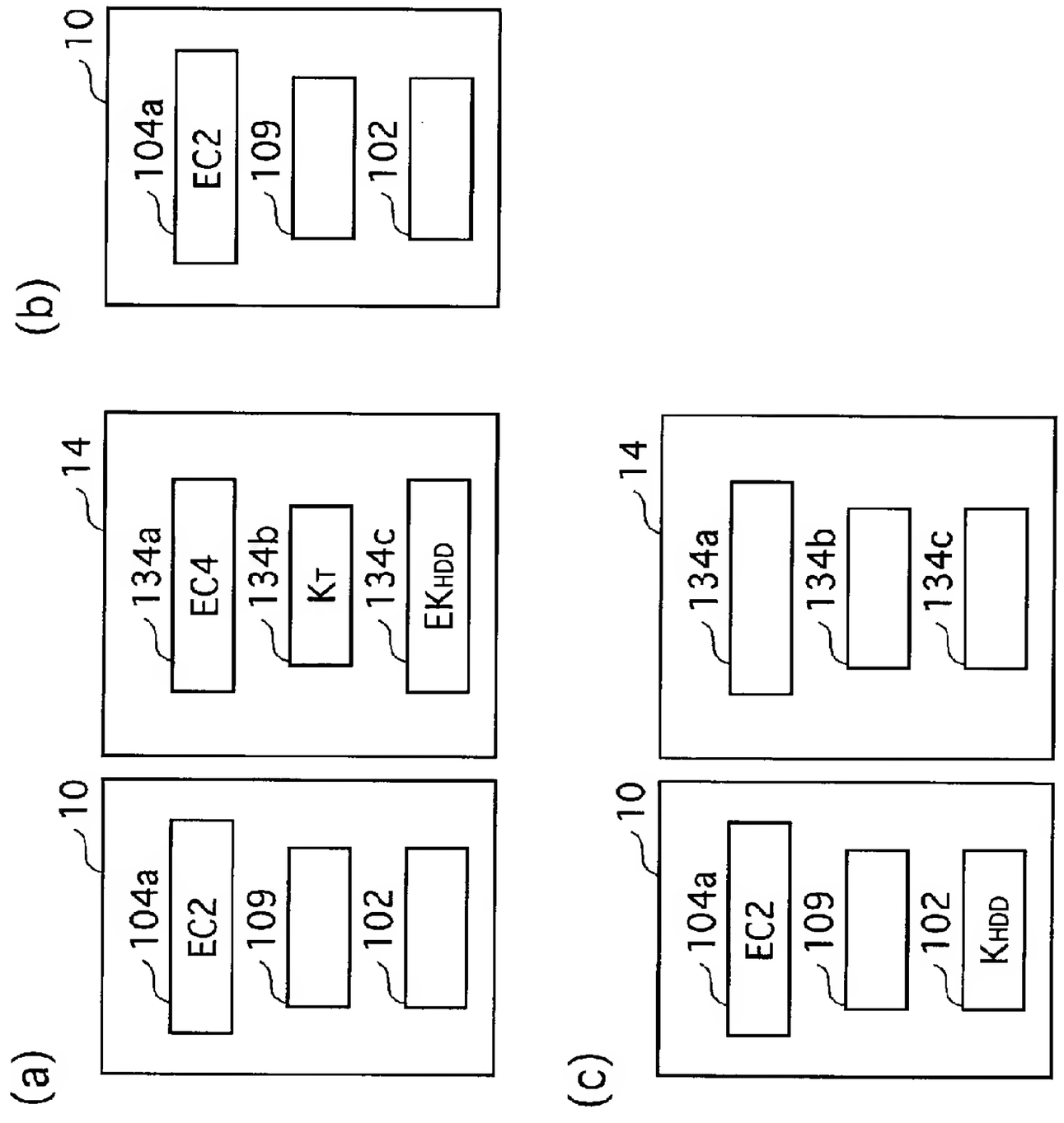

(a)
10
104a
EC2
109
KT
102
KHDD
14
134a
134b
134c
(b)
10
104a
EC2
109
KT
102
KHDD
14
134a
EC4
134b
KT
134c
EKHDD
(c)
10
104a
EC2
109
KT
102
14
134a
EC4
134b
134c
EKHDD
(d)
10
104a
EC2
109
102
14
134a
EC4
134b
KT
134c
EKHDD

[図10]

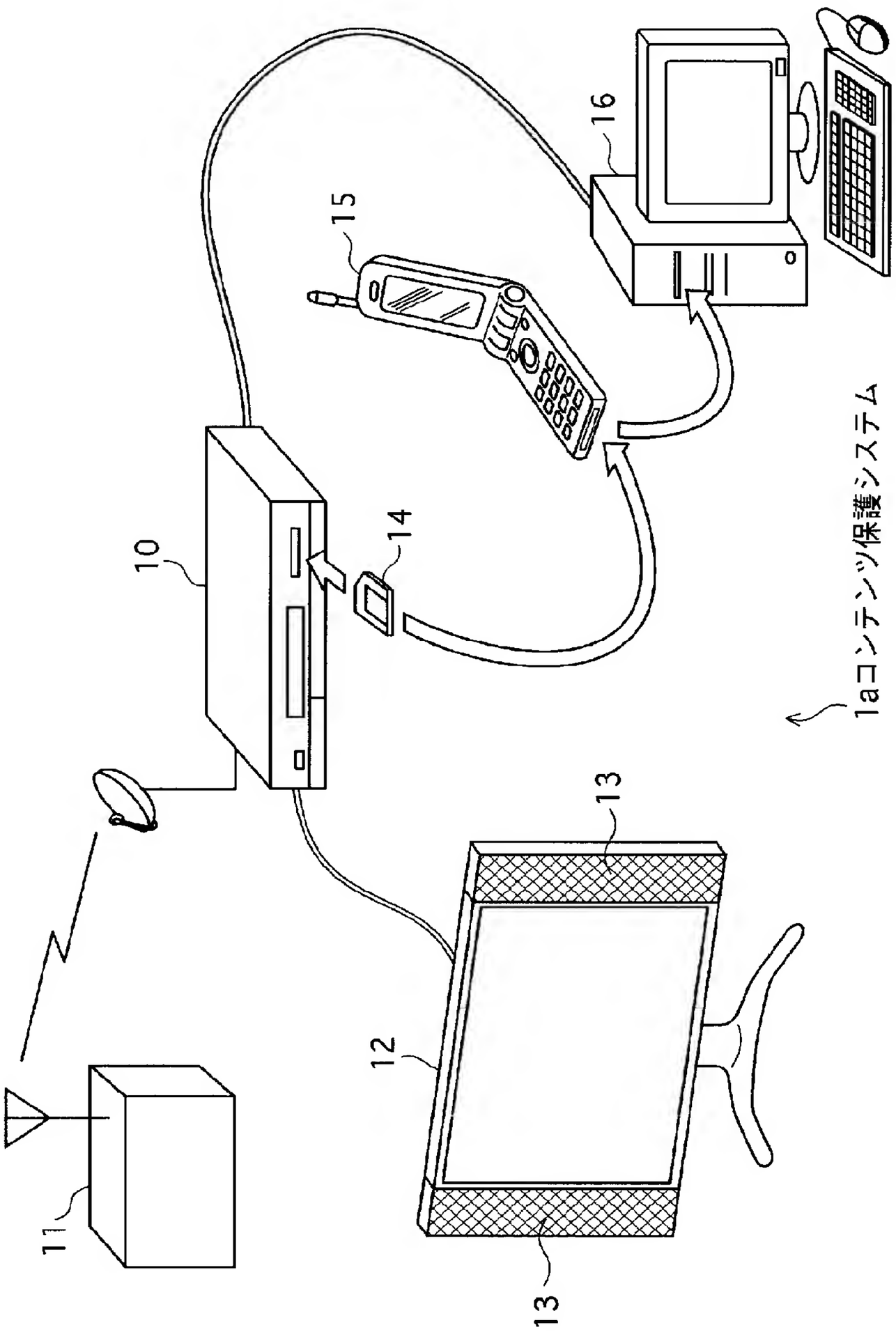

記録再生装置10
可搬媒体14
S131
KT消去
S132
EC4消去
S133
EKHDD,ID_A読出
S134
EKHDD,ID_A
S135
機器ID確認
S136
NO
OK?
YES
EKHDDをKaで復号し
KHDDを生成
S138
S137
エラー処理
END
S139
KHDD格納
RETURN
S140
EKHDD,ID_A消去
RETURN

[図11]

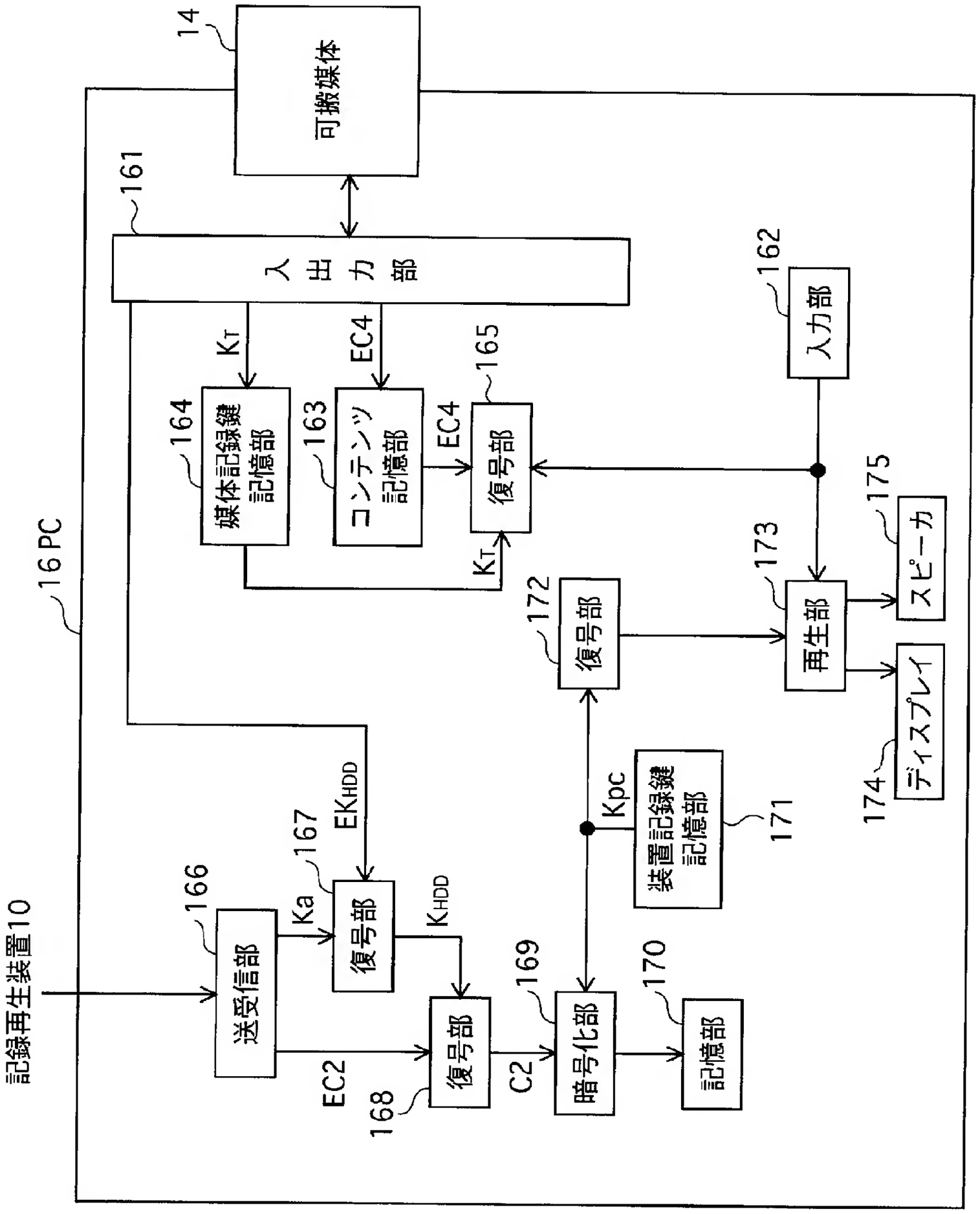

14
134a
134b
134c
EKHDD


(a)
10
104a
EC2
109
102
14
134a
EC4
134b
KT
134c
EKHDD
(b)
10
104a
EC2
109
102
14
134a
134b
134c
(c)
10
104a
EC2
109
102
KHDD
14
134a
134b
134c

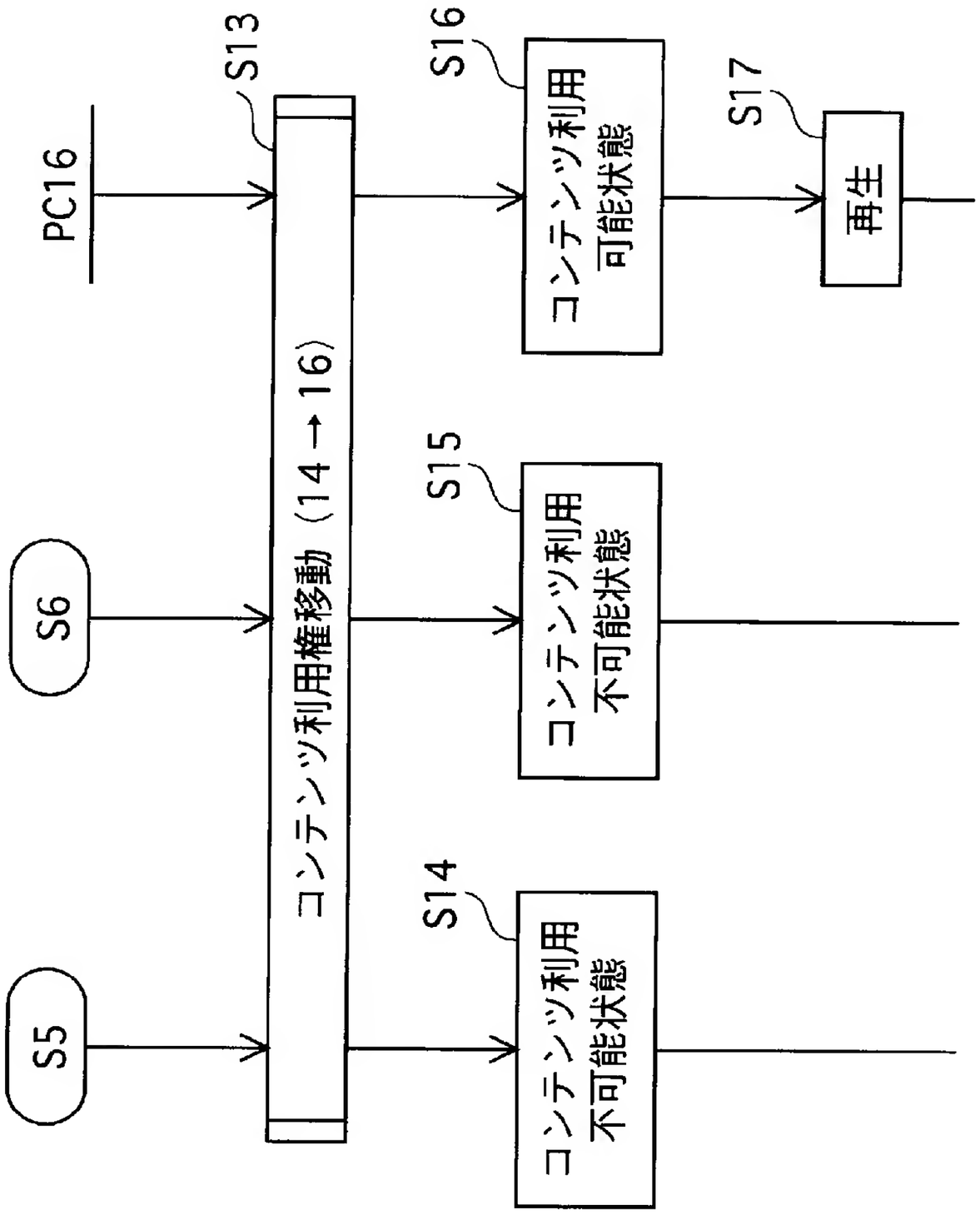
[図12]



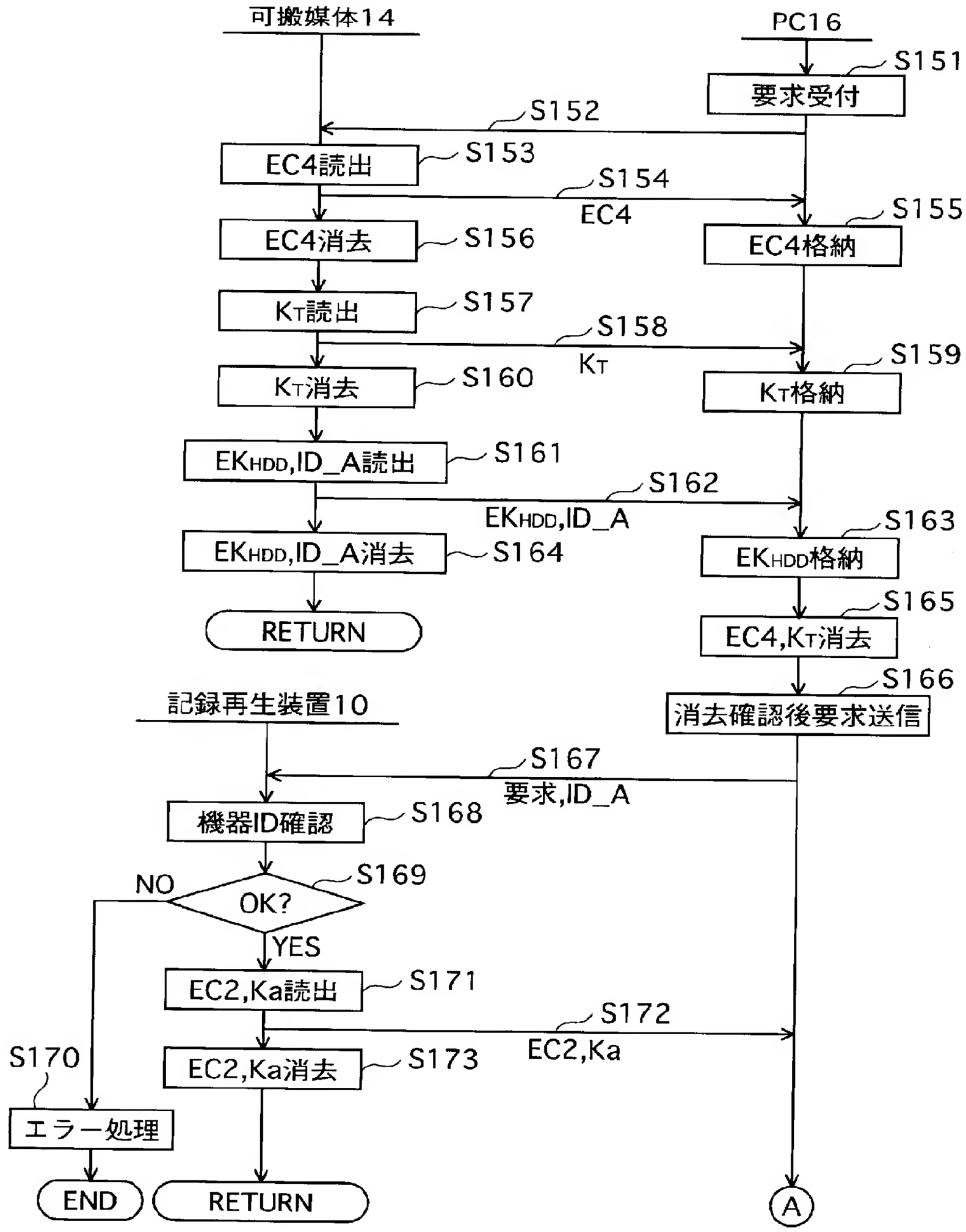
[図13]


14
可搬媒体
161
入出力部
162
入力部
K_T
EC4
165
164
媒体記録鍵記憶部
163
コンテンツ記憶部
EC4
復号部
K_T
16 PC
記録再生装置10
172
復号部
173
再生部
175
スピーカ
Kpc
装置記録鍵記憶部
171
174
ディスプレイ
EK_{HDD}
167
166
Ka
復号部
K_{HDD}
送受信部
169
170
EC2
168
復号部
C2
暗号化部
記憶部

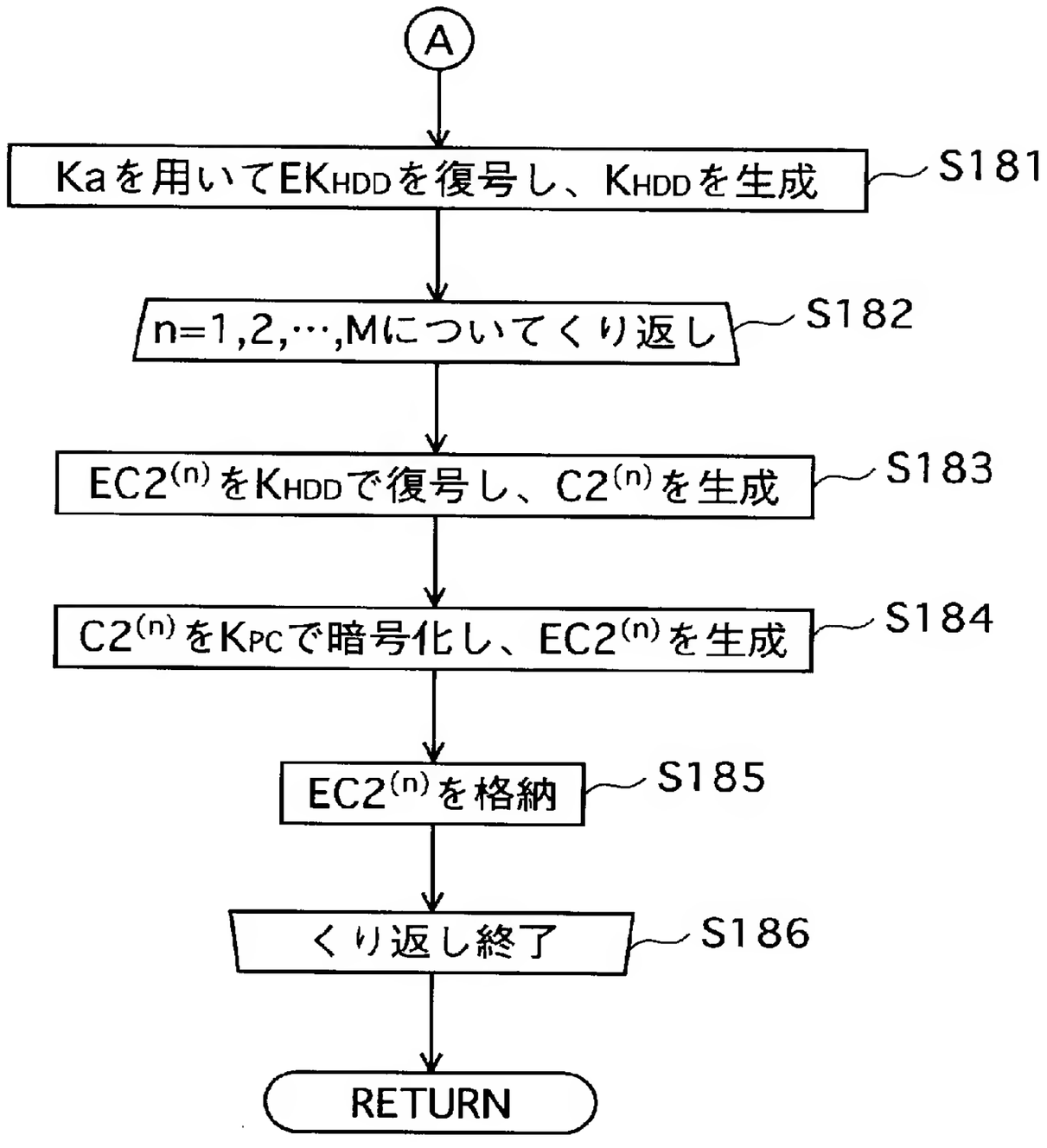
[図14]


PC16
S13
S16
S17
コンテンツ利用
可能状態
再生
S6
S5
コンテンツ利用権移動（14→16）
S15
コンテンツ利用
不可能状態
S14
コンテンツ利用
不可能状態

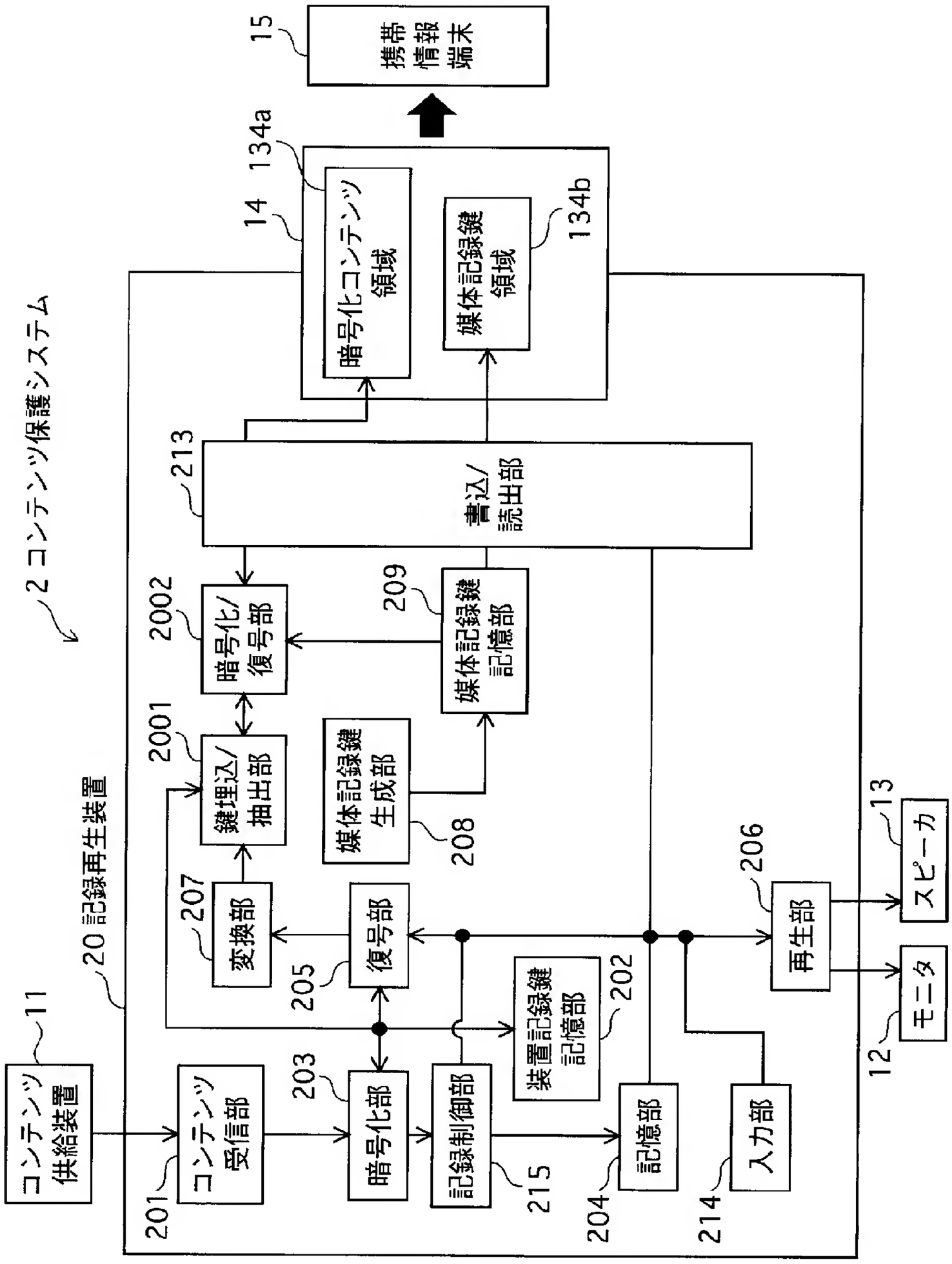
[図15]


可搬媒体14
PC16
S151
要求受付
S152
EC4読出
S153
S154
EC4
S155
EC4消去
S156
EC4格納
KT読出
S157
S158
KT
S159
KT消去
S160
KT格納
EKHDD,ID_A読出
S161
S162
EKHDD,ID_A
S163
EKHDD,ID_A消去
S164
EKHDD格納
RETURN
S165
EC4,KT消去
S166
消去確認後要求送信
記録再生装置10
S167
要求,ID_A
機器ID確認
S168
NO
OK?
S169
YES
EC2,Ka読出
S171
S172
EC2,Ka
S170
EC2,Ka消去
S173
エラー処理
END
RETURN
A

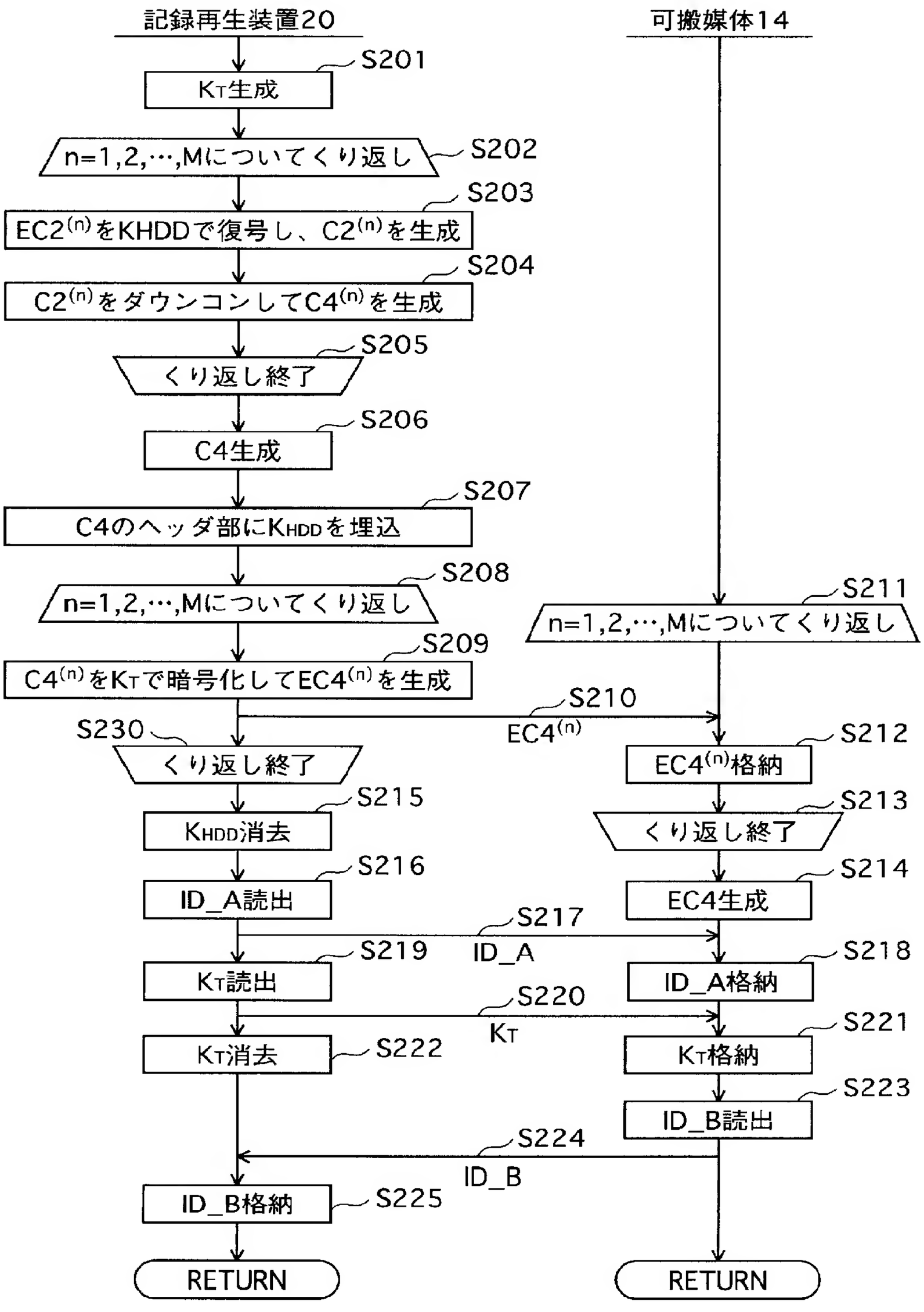
[図16]


A
Kaを用いてEKHDDを復号し、KHDDを生成
S181
n=1,2,…,Mについてくり返し
S182
EC2(n)をKHDDで復号し、C2(n)を生成
S183
C2(n)をKPCで暗号化し、EC2(n)を生成
S184
EC2(n)を格納
S185
くり返し終了
S186
RETURN

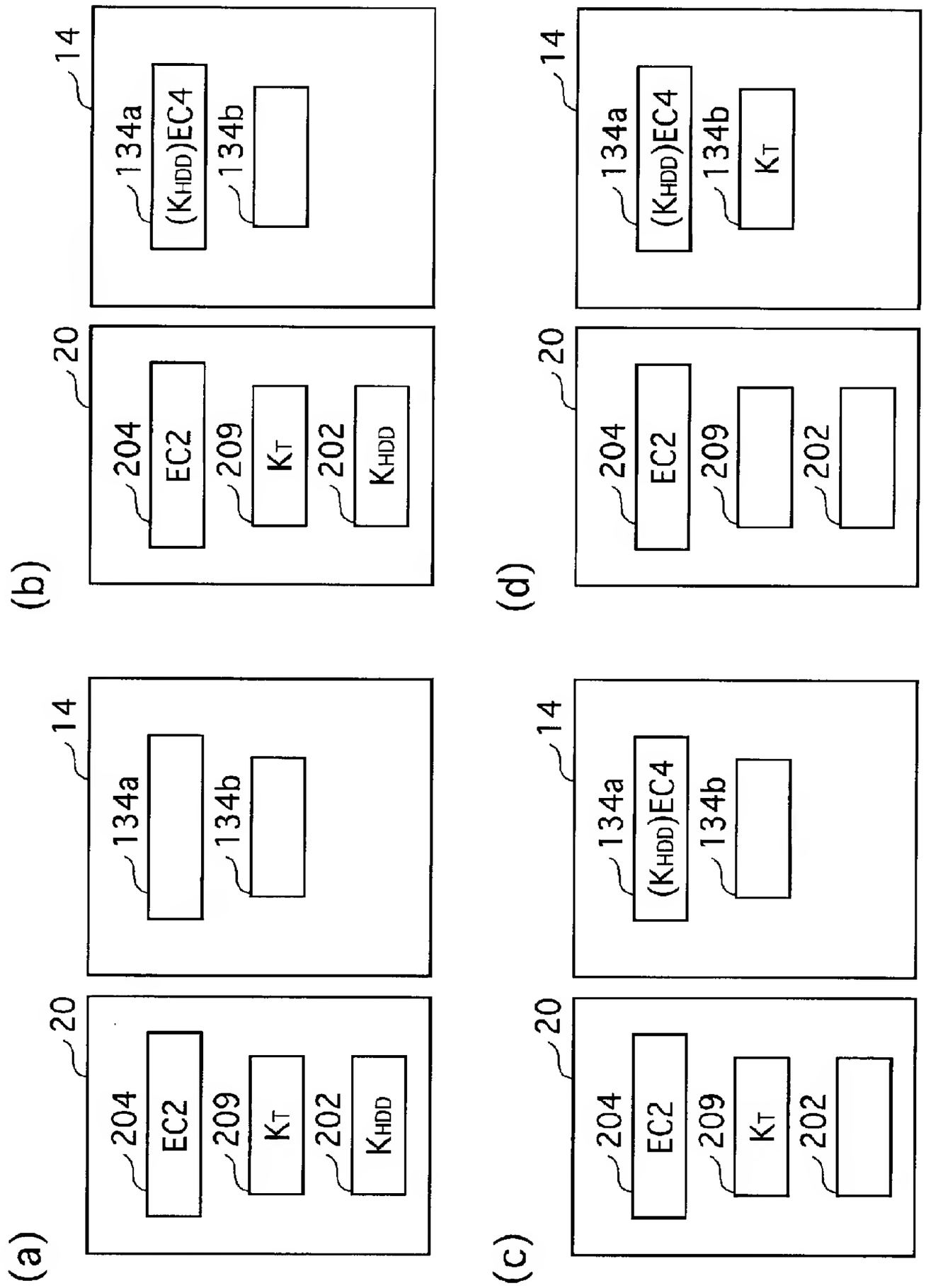
[図17]


2 コンテンツ保護システム
20 記録再生装置
11
コンテンツ供給装置
201
コンテンツ受信部
203
暗号化部
記録制御部
215
204
記憶部
214
入力部
202
装置記録鍵記憶部
205
復号部
207
変換部
206
再生部
13
スピーカ
モニタ
12
2001
鍵埋込/抽出部
2002
暗号化/復号部
213
書込/読出部
209
媒体記録鍵記憶部
208
媒体記録鍵生成部
14
134a
暗号化コンテンツ領域
134b
媒体記録鍵領域
15
携帯情報端末

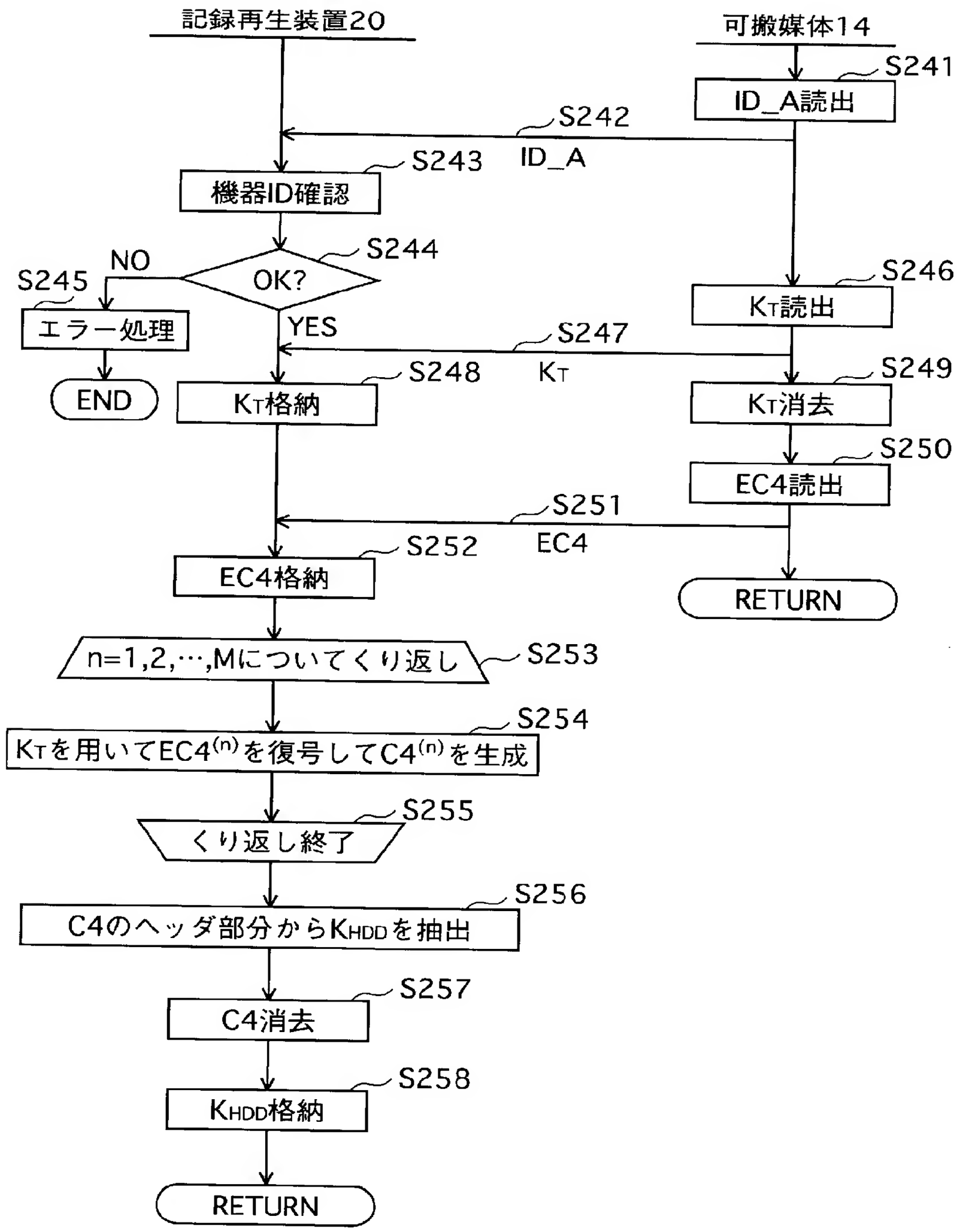
[図18]


記録再生装置20
可搬媒体14
S201
KT生成
S202
n=1,2,…,Mについてくり返し
S203
EC2(n)をKHDDで復号し、C2(n)を生成
S204
C2(n)をダウンコンしてC4(n)を生成
S205
くり返し終了
S206
C4生成
S207
C4のヘッダ部にKHDDを埋込
S208
n=1,2,…,Mについてくり返し
S209
C4(n)をKTで暗号化してEC4(n)を生成
S210
EC4(n)
S211
n=1,2,…,Mについてくり返し
S230
くり返し終了
S212
EC4(n)格納
S215
KHDD消去
S213
くり返し終了
S216
ID_A読出
S214
EC4生成
S217
ID_A
S219
KT読出
S218
ID_A格納
S220
KT
S221
KT格納
S222
KT消去
S223
ID_B読出
S224
ID_B
S225
ID_B格納
RETURN
RETURN

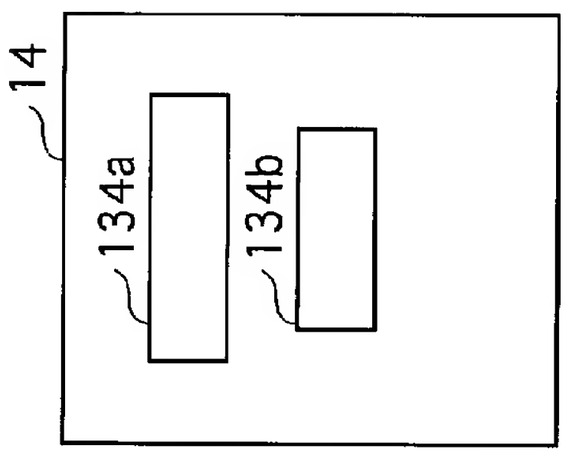
[図19]

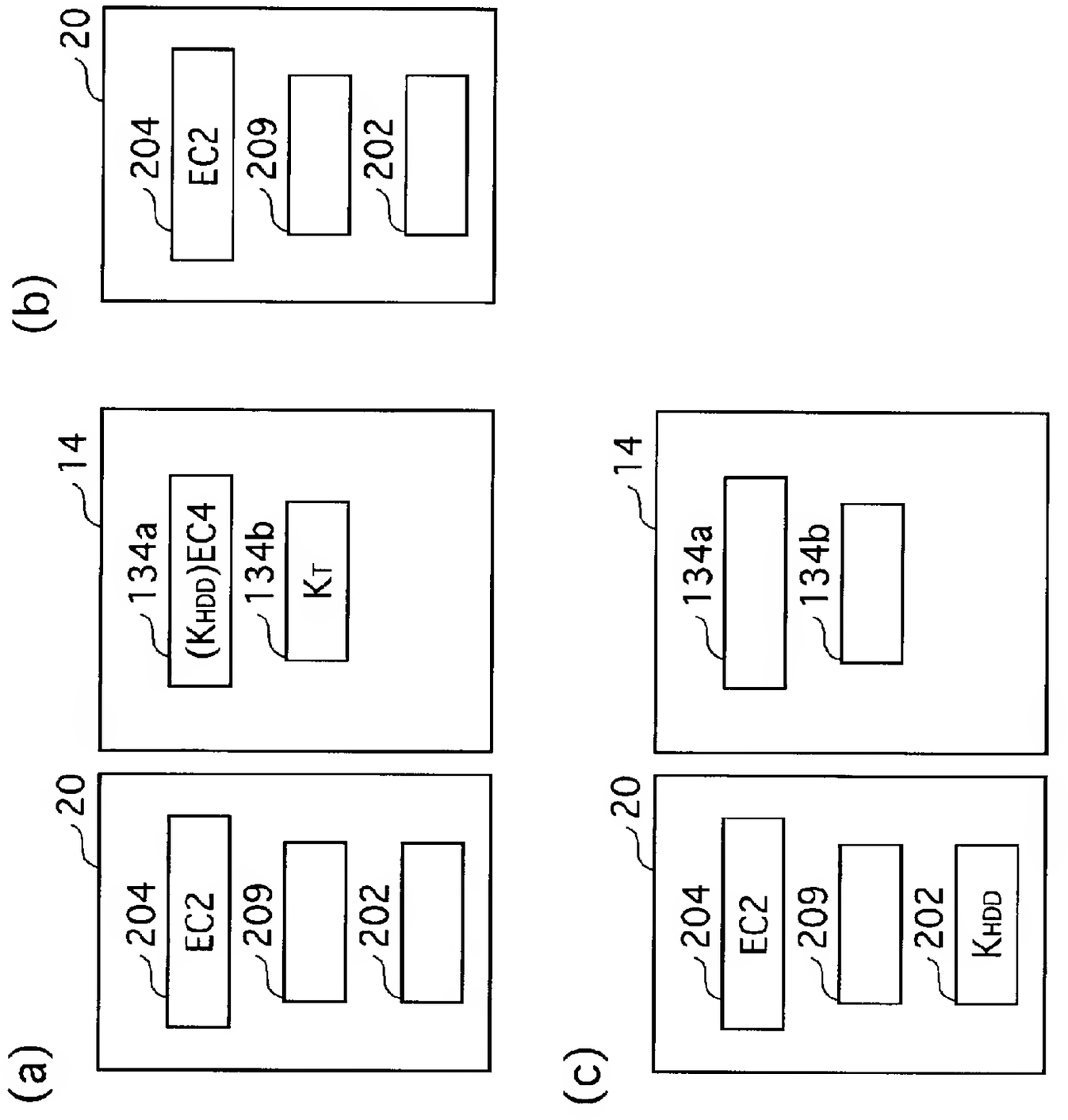

(a)
20
204
EC2
209
K_T
202
K_{HDD}
14
134a
134b
(b)
20
204
EC2
209
K_T
202
K_{HDD}
14
134a
$(K_{HDD})EC4$
134b
(c)
20
204
EC2
209
K_T
202
14
134a
$(K_{HDD})EC4$
134b
(d)
20
204
EC2
209
202
14
134a
$(K_{HDD})EC4$
134b
K_T

[図20]

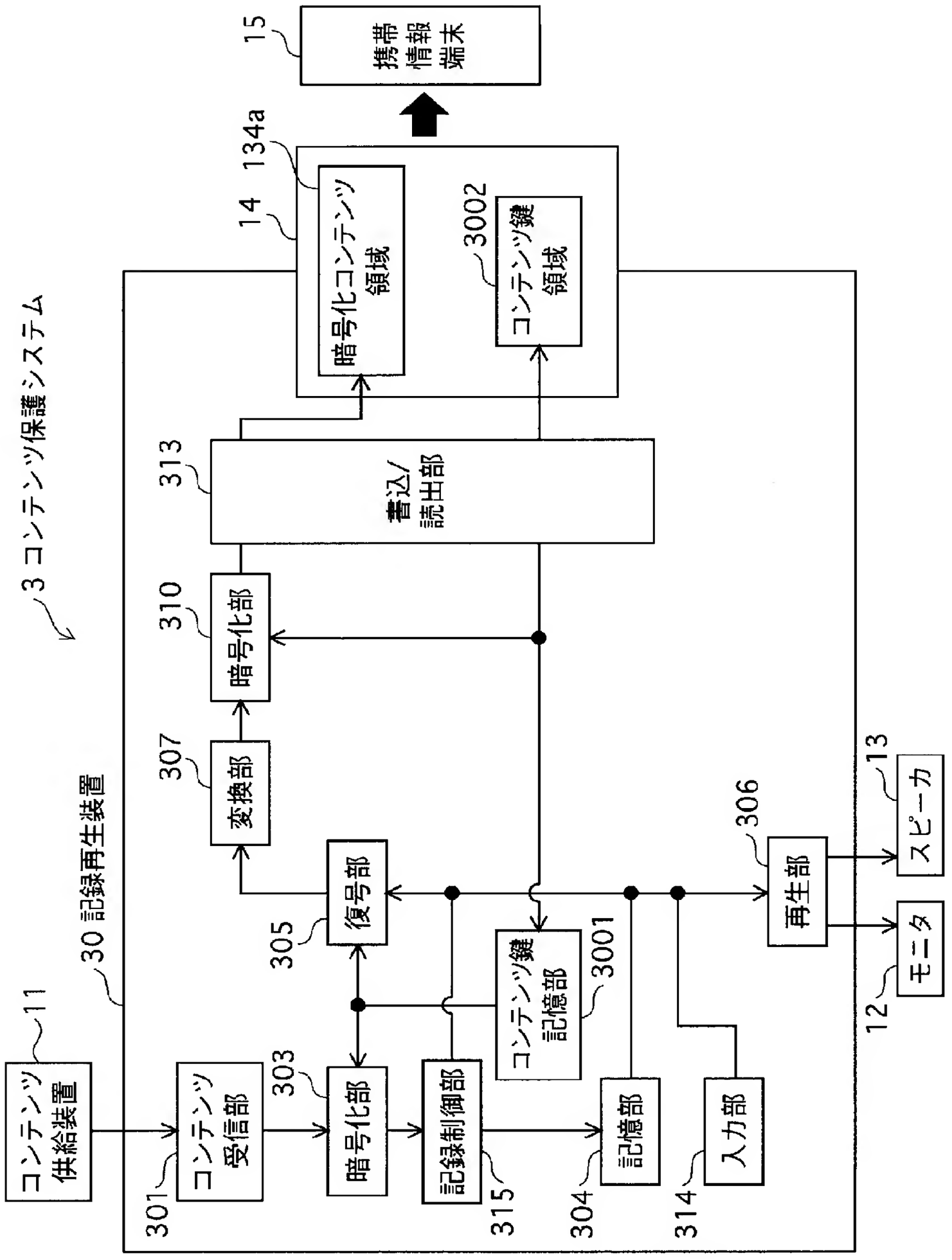

記録再生装置20
可搬媒体14
S241
ID_A読出
S242
ID_A
S243
機器ID確認
S244
OK?
NO
S245
エラー処理
END
YES
S246
KT読出
S247
KT
S248
KT格納
S249
KT消去
S250
EC4読出
S251
EC4
S252
EC4格納
RETURN
n=1,2,…,Mについてくり返し
S253
S254
KTを用いてEC4(n)を復号してC4(n)を生成
S255
くり返し終了
S256
C4のヘッダ部分からKHDDを抽出
S257
C4消去
S258
KHDD格納
RETURN

[図21]

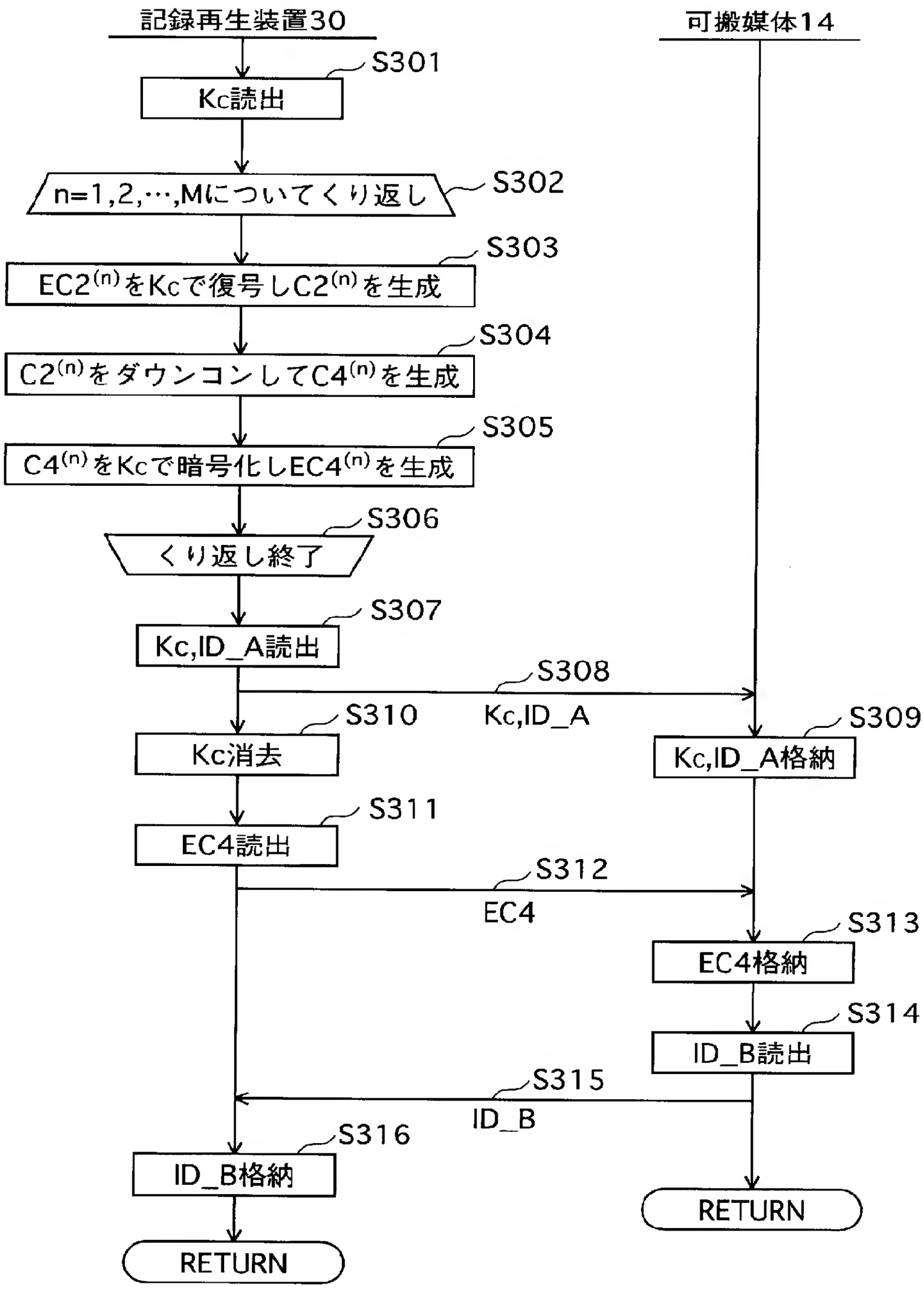

14
134a
134b


(a)
20
204
EC2
209
202
14
134a
(KHDD)EC4
134b
KT
(b)
20
204
EC2
209
202
14
134a
134b
(c)
20
204
EC2
209
202
KHDD
14
134a
134b

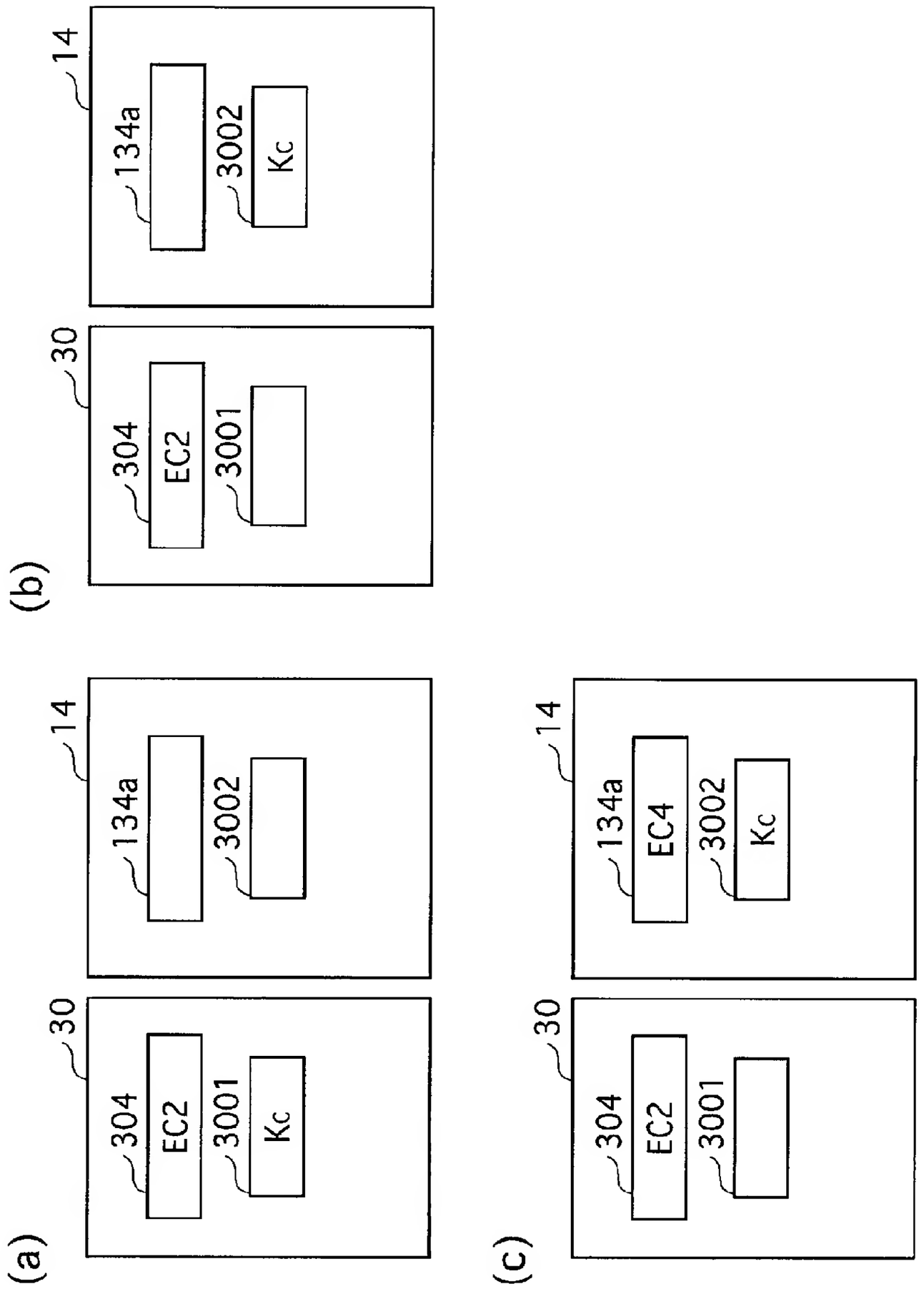
[図22]


3 コンテンツ保護システム
30 記録再生装置
11
コンテンツ供給装置
301
コンテンツ受信部
303
暗号化部
305
復号部
307
変換部
310
暗号化部
313
書込/読出部
14
134a
暗号化コンテンツ領域
3002
コンテンツ鍵領域
15
携帯情報端末
3001
コンテンツ鍵記憶部
306
再生部
13
スピーカ
12
モニタ
315
記録制御部
304
記憶部
314
入力部

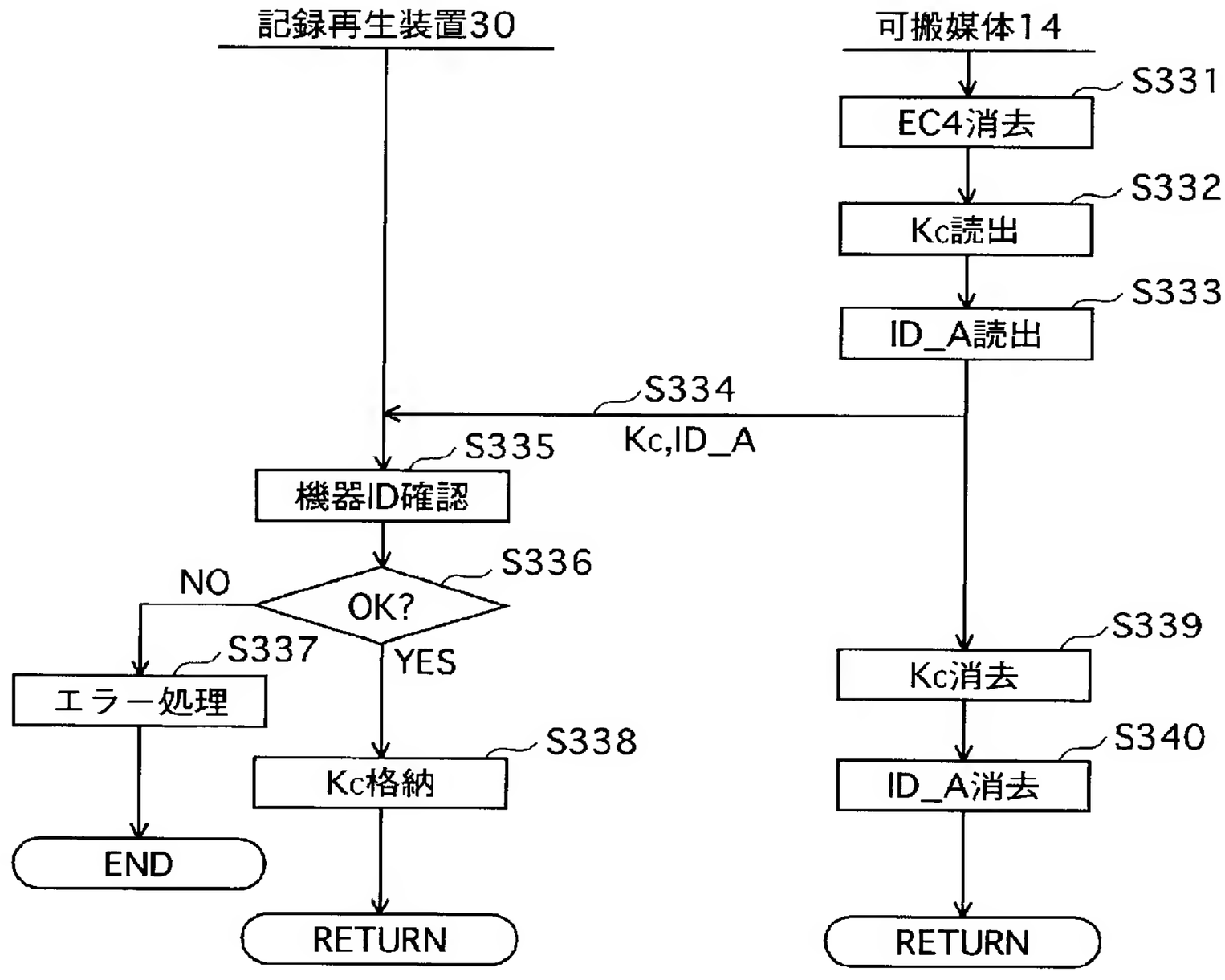
[図23]


記録再生装置30
可搬媒体14
S301
Kc読出
S302
n=1,2,…,Mについてくり返し
S303
EC2(n)をKcで復号しC2(n)を生成
S304
C2(n)をダウンコンしてC4(n)を生成
S305
C4(n)をKcで暗号化しEC4(n)を生成
S306
くり返し終了
S307
Kc,ID_A読出
S308
Kc,ID_A
S309
Kc,ID_A格納
S310
Kc消去
S311
EC4読出
S312
EC4
S313
EC4格納
S314
ID_B読出
S315
ID_B
S316
ID_B格納
RETURN
RETURN

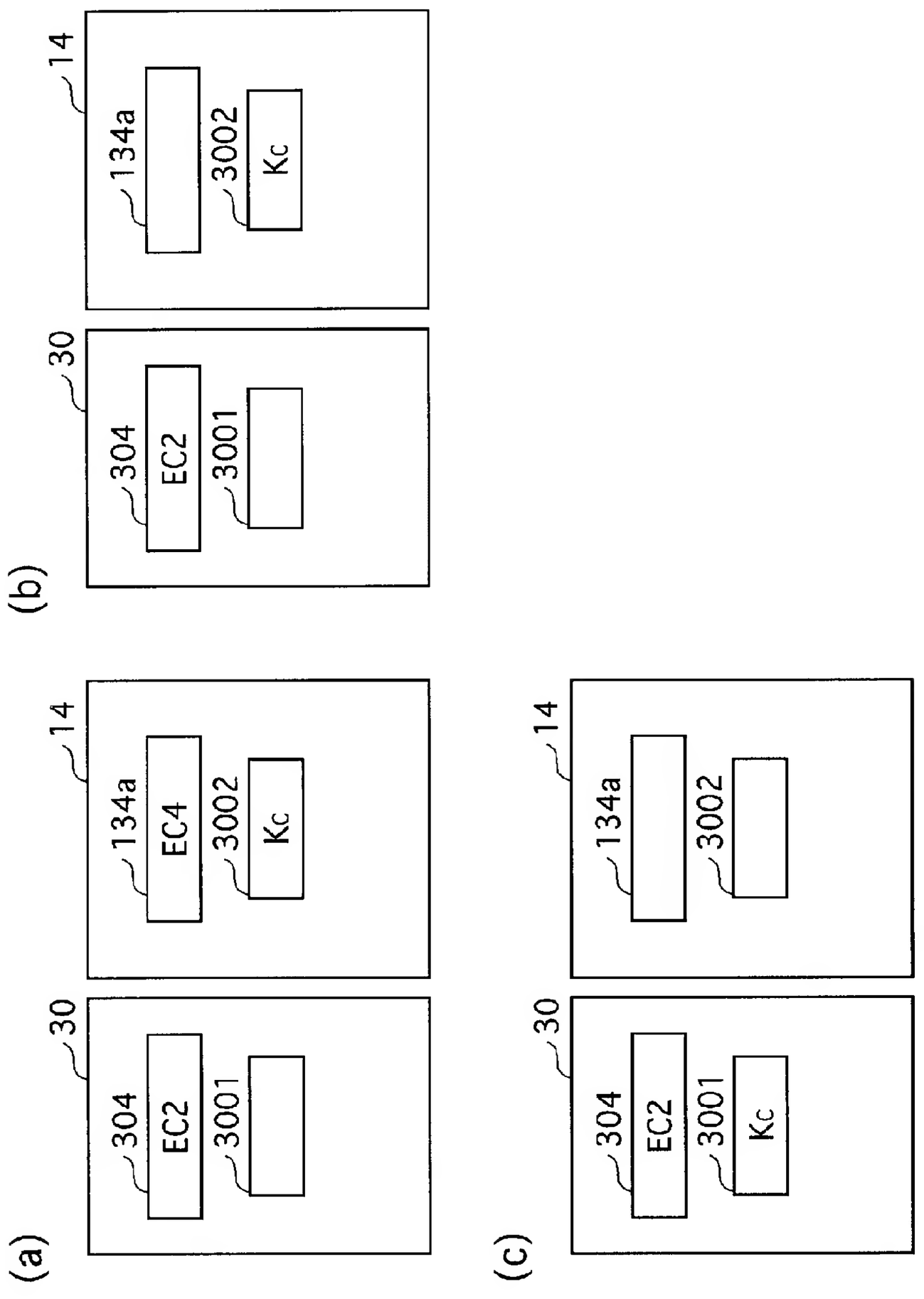
[図24]


(a)
30
304
EC2
3001
Kc
14
134a
3002
(b)
30
304
EC2
3001
14
134a
3002
(c)
30
304
EC2
3001
14
134a
EC4
3002
Kc

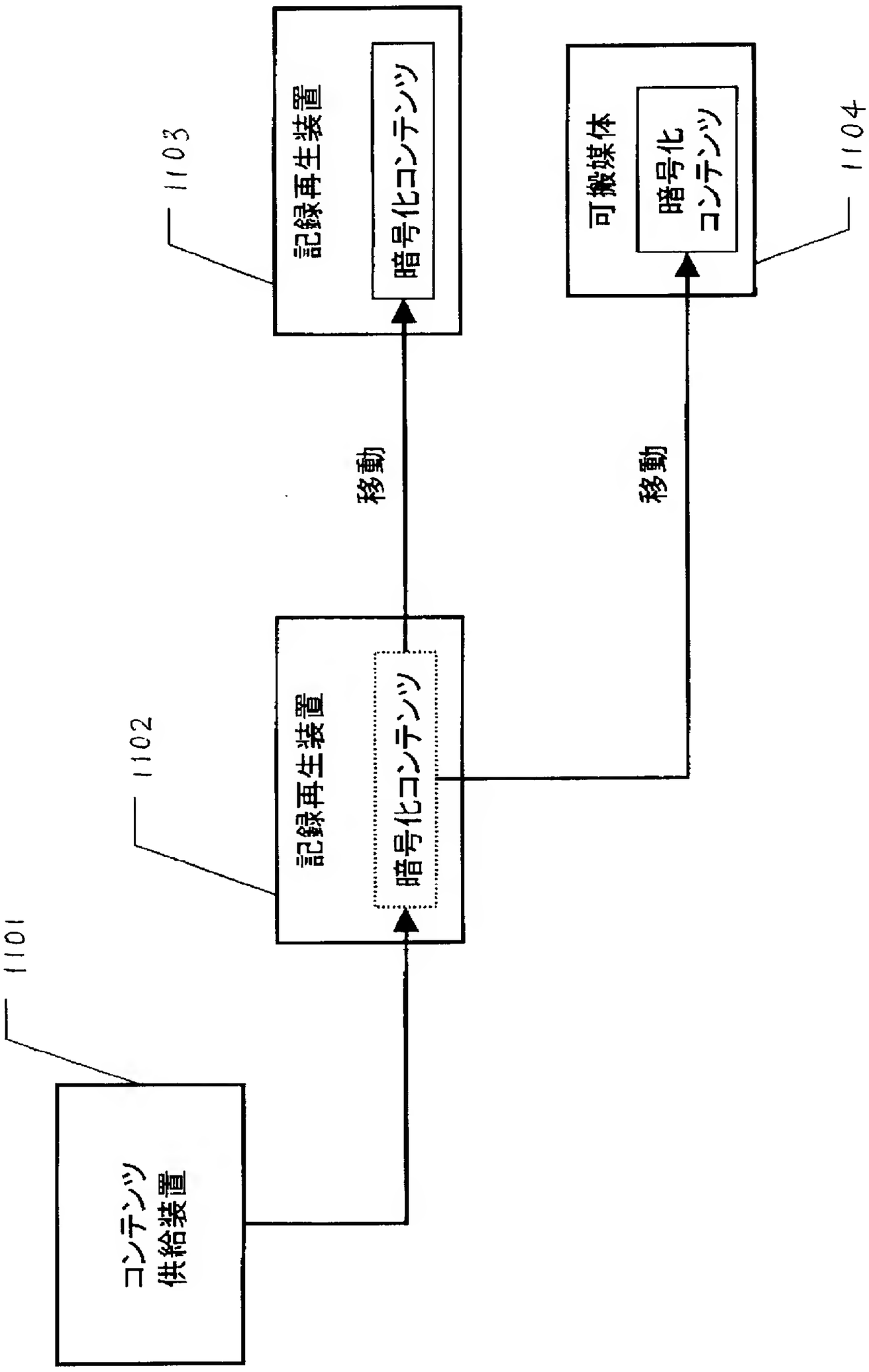
[図25]


記録再生装置30
可搬媒体14
S331
EC4消去
S332
Kc読出
S333
ID_A読出
S334
Kc,ID_A
S335
機器ID確認
S336
OK?
NO
YES
S337
エラー処理
S338
Kc格納
END
RETURN
S339
Kc消去
S340
ID_A消去
RETURN

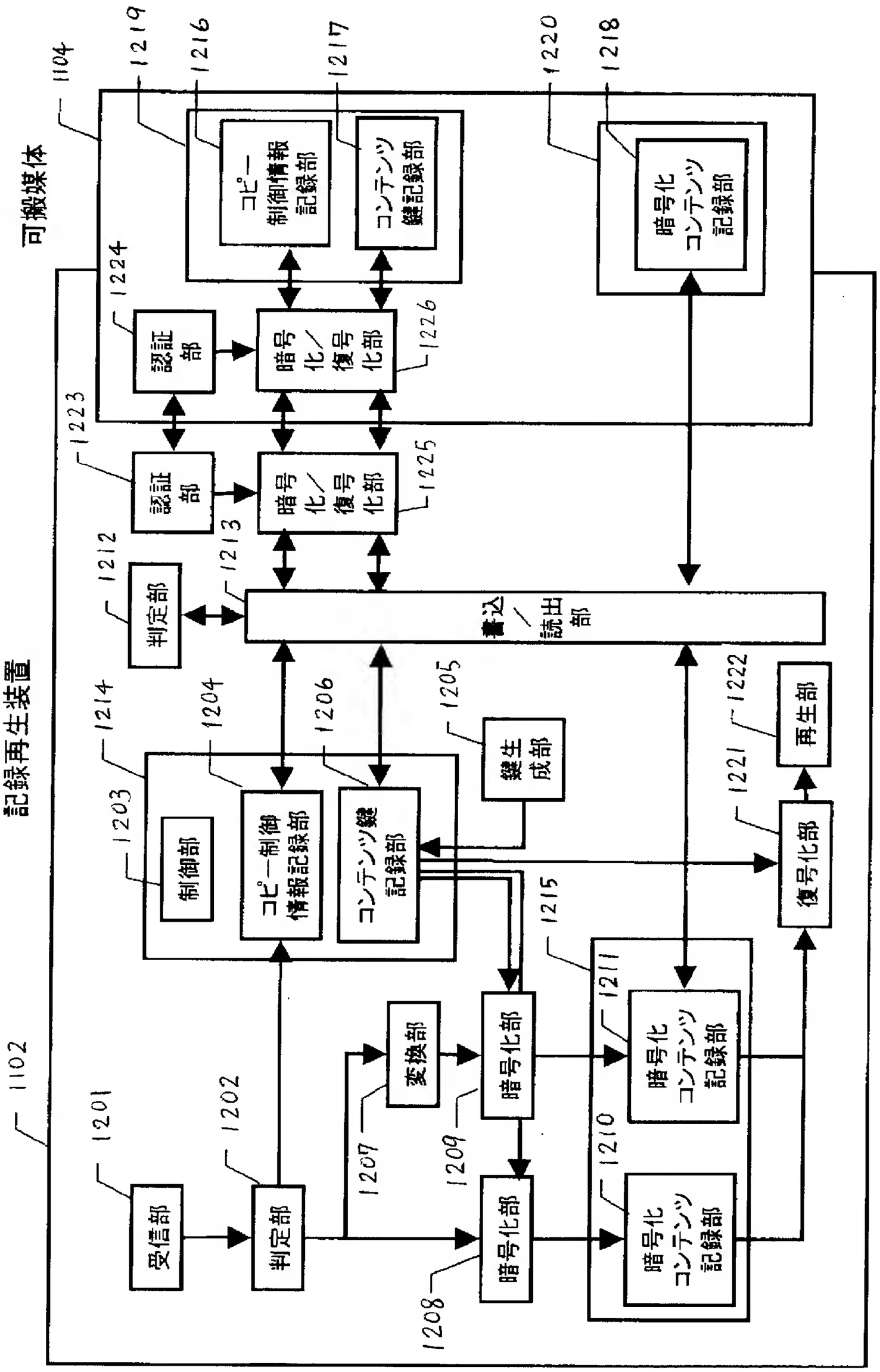
[図26]


14
134a
3002
Kc
(b)
30
304
EC2
3001
14
134a
EC4
3002
Kc
(a)
30
304
EC2
3001
(c)
14
134a
3002
30
304
EC2
3001
Kc

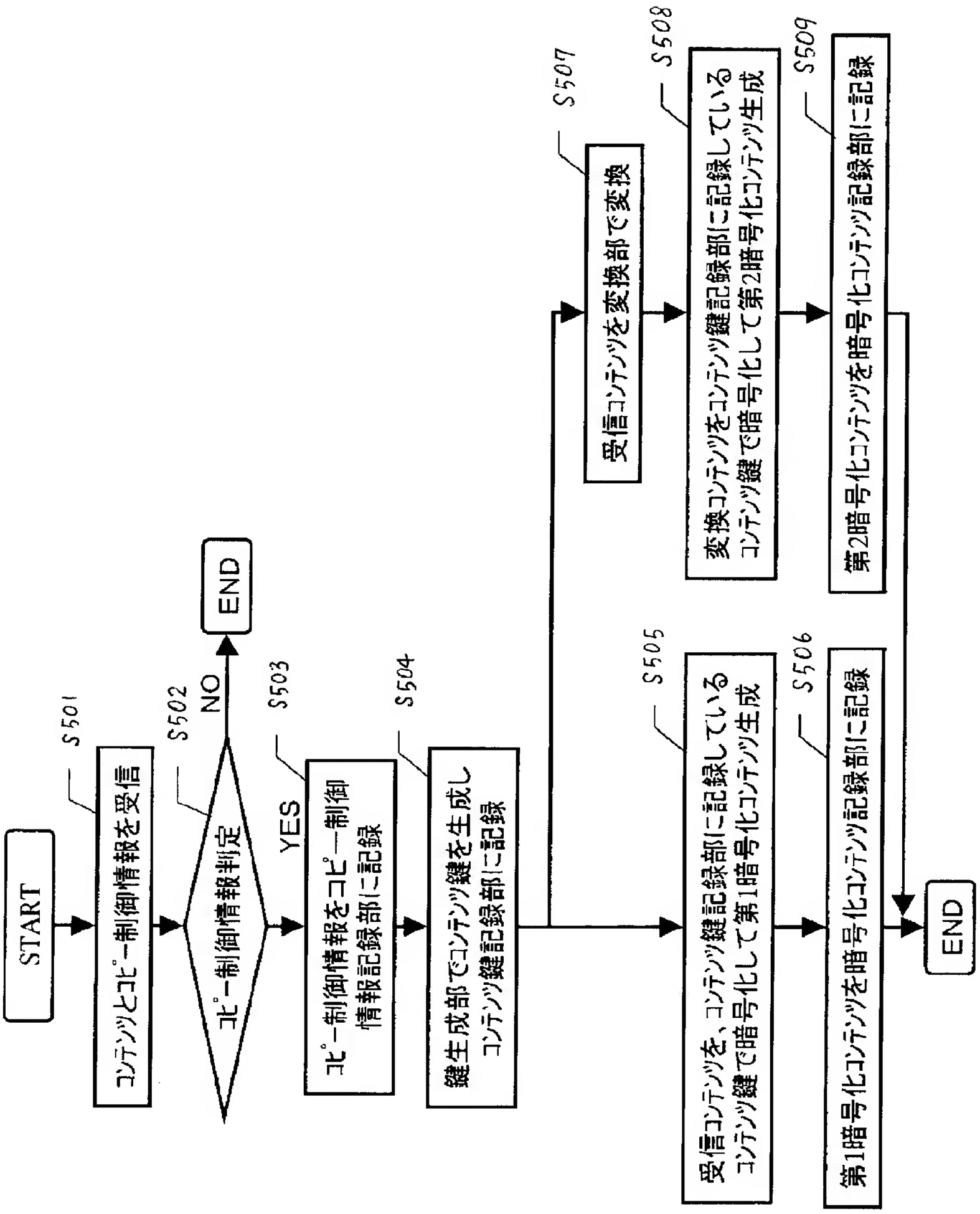
[図27]


1103
記録再生装置
暗号化コンテンツ
可搬媒体
暗号化
コンテンツ
1104
移動
移動
1102
記録再生装置
暗号化コンテンツ
1101
コンテンツ
供給装置

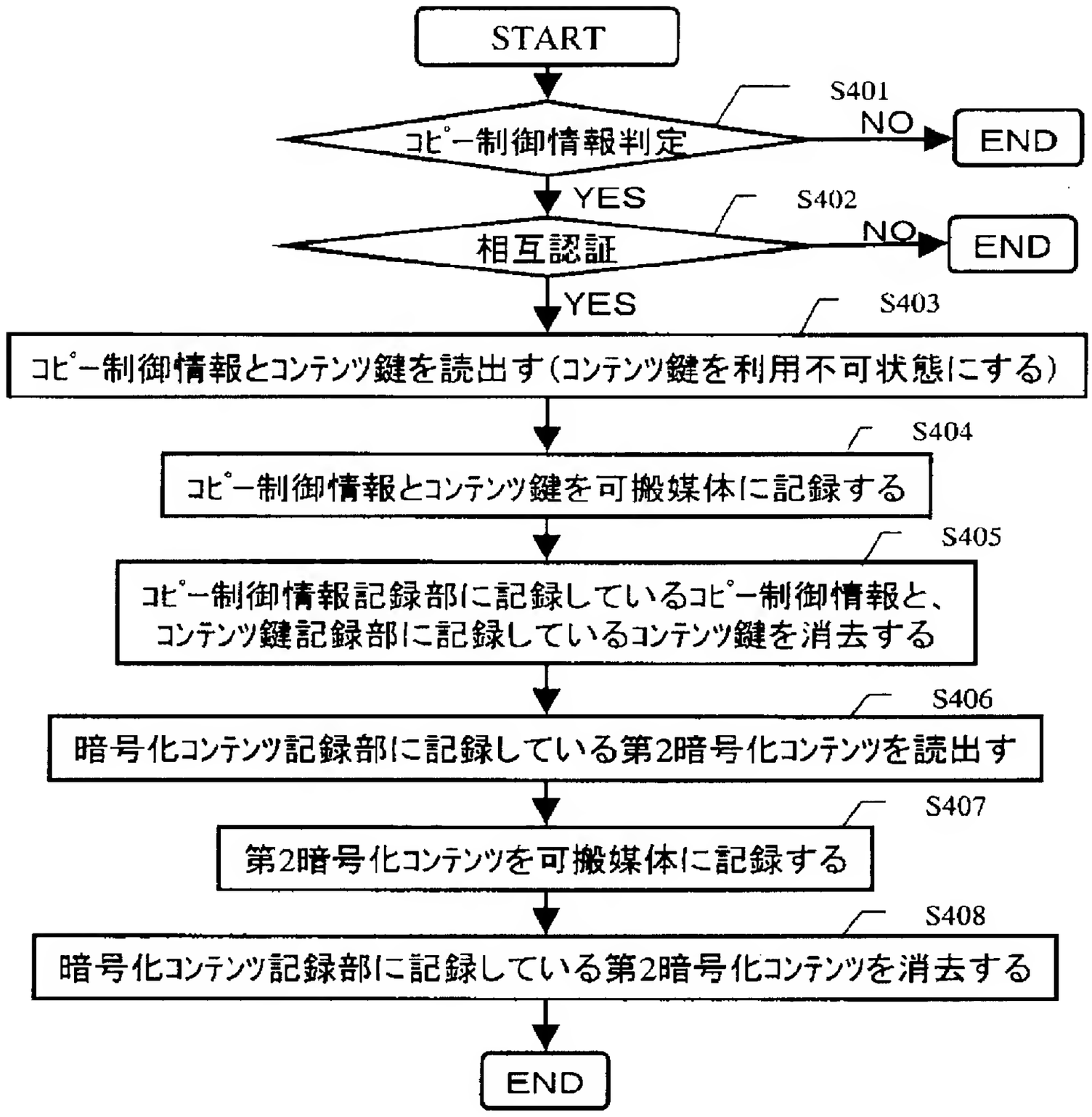
[図28]


記録再生装置
1102
可搬媒体
1104
1201
受信部
1202
判定部
1203
制御部
1204
コピー制御情報記録部
1205
鍵生成部
1206
コンテンツ鍵記録部
1207
変換部
1208
暗号化部
1209
暗号化部
1210
暗号化コンテンツ記録部
1211
暗号化コンテンツ記録部
1212
判定部
1213
書込／読出部
1214
1215
1216
コピー制御情報記録部
1217
コンテンツ鍵記録部
1218
暗号化コンテンツ記録部
1219
1220
1221
復号化部
1222
再生部
1223
認証部
1224
認証部
1225
暗号化／復号化部
1226
暗号化／復号化部

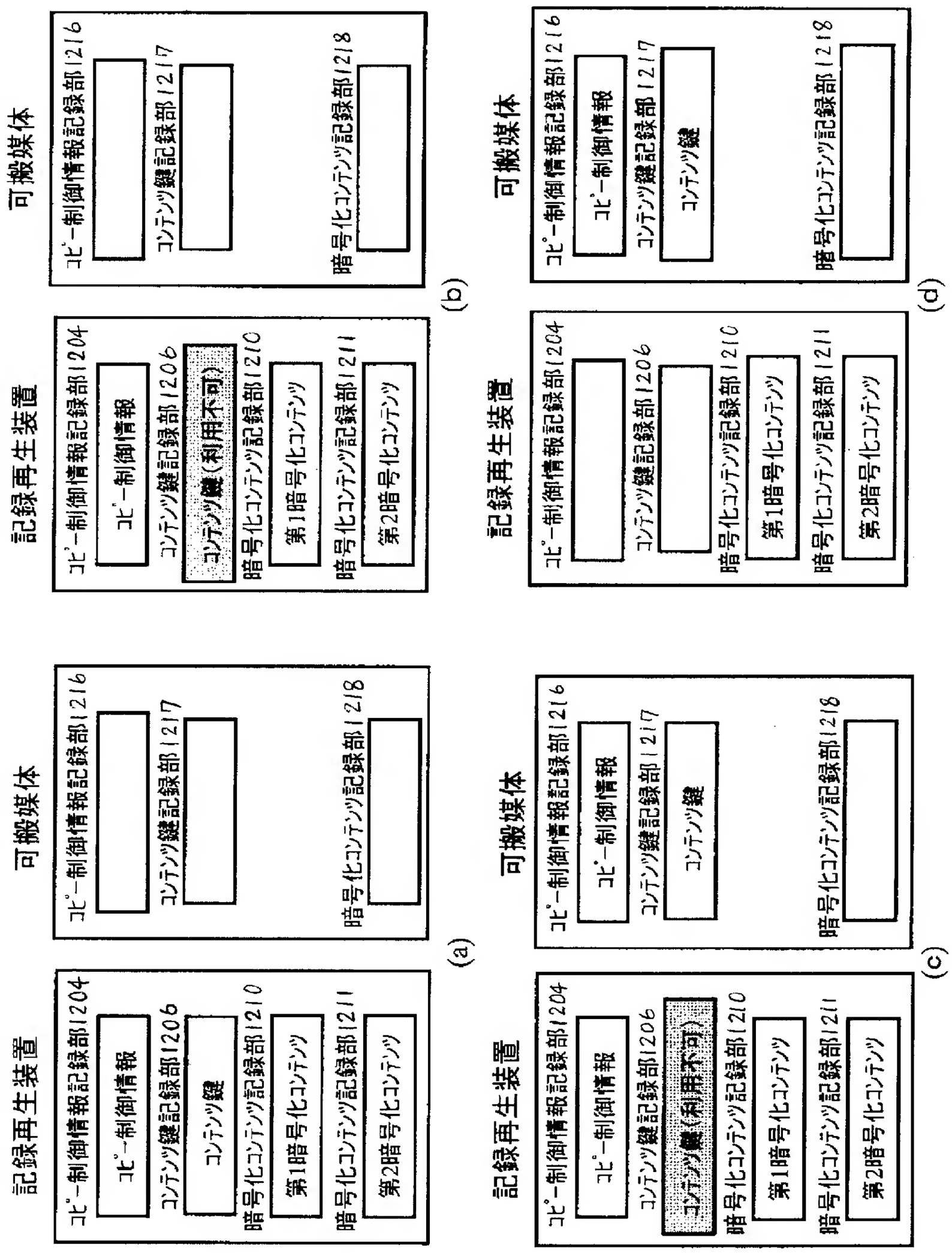
[図29]


START
S501
コンテンツとコピー制御情報を受信
S502
コピー制御情報判定
NO
END
YES
S503
コピー制御情報をコピー制御情報記録部に記録
S504
鍵生成部でコンテンツ鍵を生成しコンテンツ鍵記録部に記録
S505
受信コンテンツを、コンテンツ鍵記録部に記録しているコンテンツ鍵で暗号化して第1暗号化コンテンツ生成
S506
第1暗号化コンテンツを暗号化コンテンツ記録部に記録
S507
受信コンテンツを変換部で変換
S508
変換コンテンツをコンテンツ鍵記録部に記録しているコンテンツ鍵で暗号化して第2暗号化コンテンツ生成
S509
第2暗号化コンテンツを暗号化コンテンツ記録部に記録
END

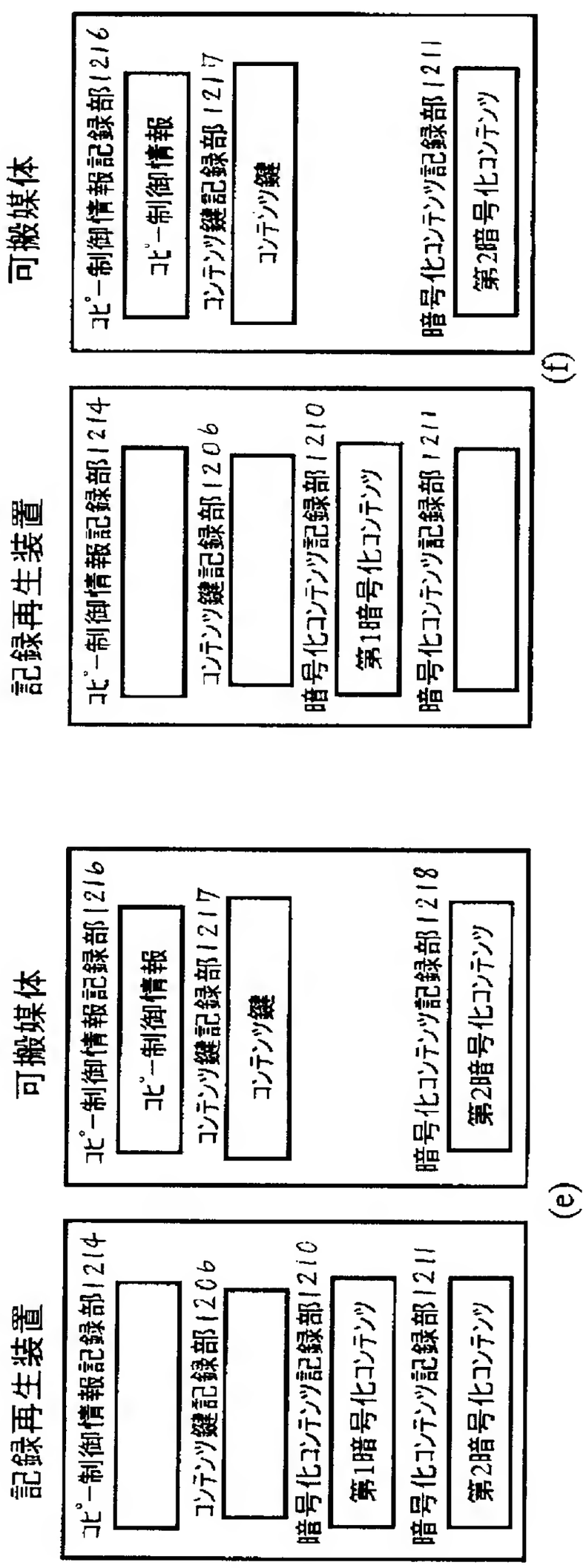
[図30]


START
S401
コピー制御情報判定
NO
END
YES
S402
相互認証
NO
END
YES
S403
コピー制御情報とコンテンツ鍵を読出す(コンテンツ鍵を利用不可状態にする)
S404
コピー制御情報とコンテンツ鍵を可搬媒体に記録する
S405
コピー制御情報記録部に記録しているコピー制御情報と、
コンテンツ鍵記録部に記録しているコンテンツ鍵を消去する
S406
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S407
第2暗号化コンテンツを可搬媒体に記録する
S408
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

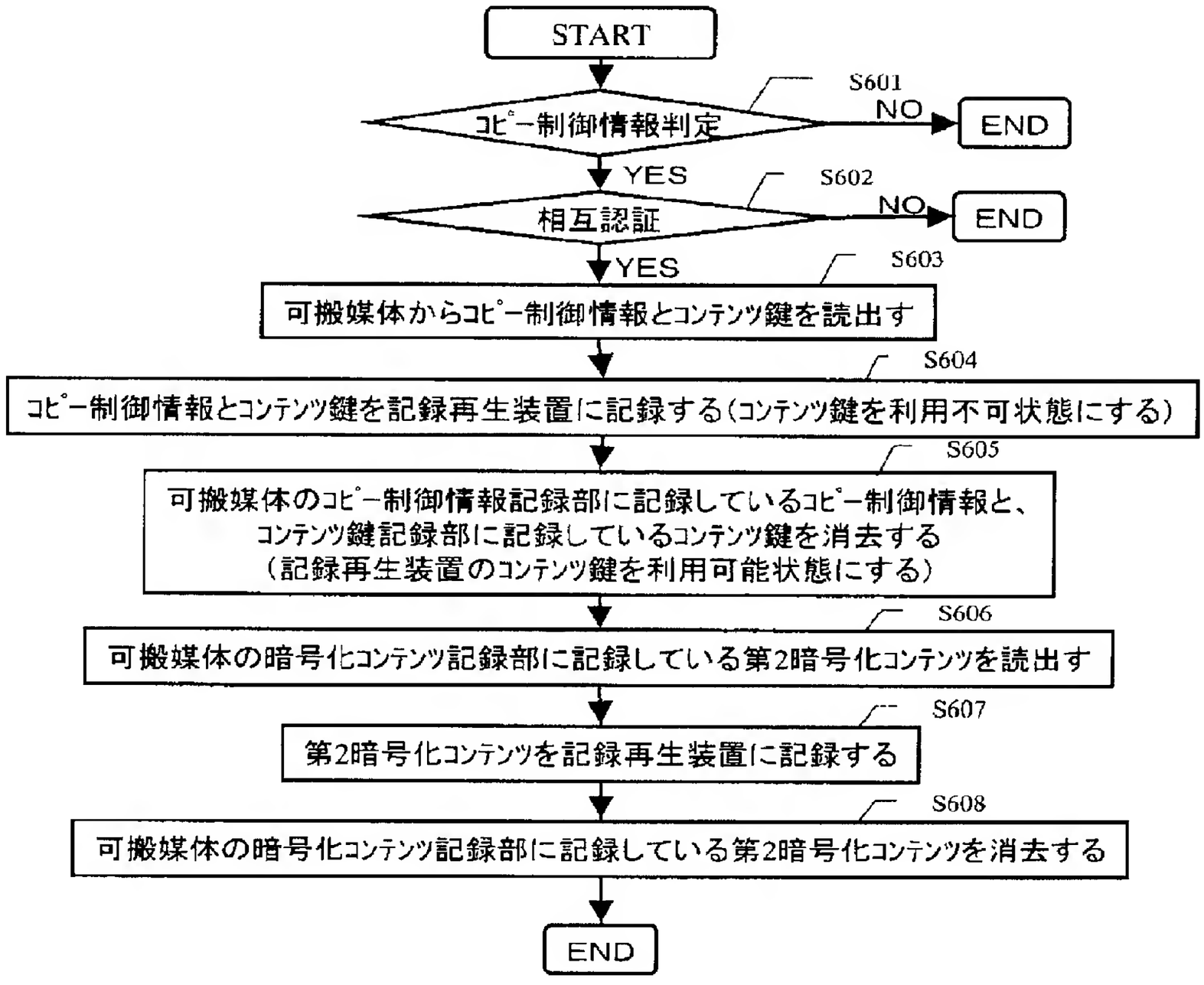
[図31]


可搬媒体
コピー制御情報記録部1216
コンテンツ鍵記録部1217
暗号化コンテンツ記録部1218
(a)
記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1206
コンテンツ鍵(利用不可)
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
第2暗号化コンテンツ
(b)
可搬媒体
コピー制御情報記録部1216
コピー制御情報
コンテンツ鍵記録部1217
コンテンツ鍵
暗号化コンテンツ記録部1218
(c)
記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1206
コンテンツ鍵(利用不可)
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
第2暗号化コンテンツ
(d)

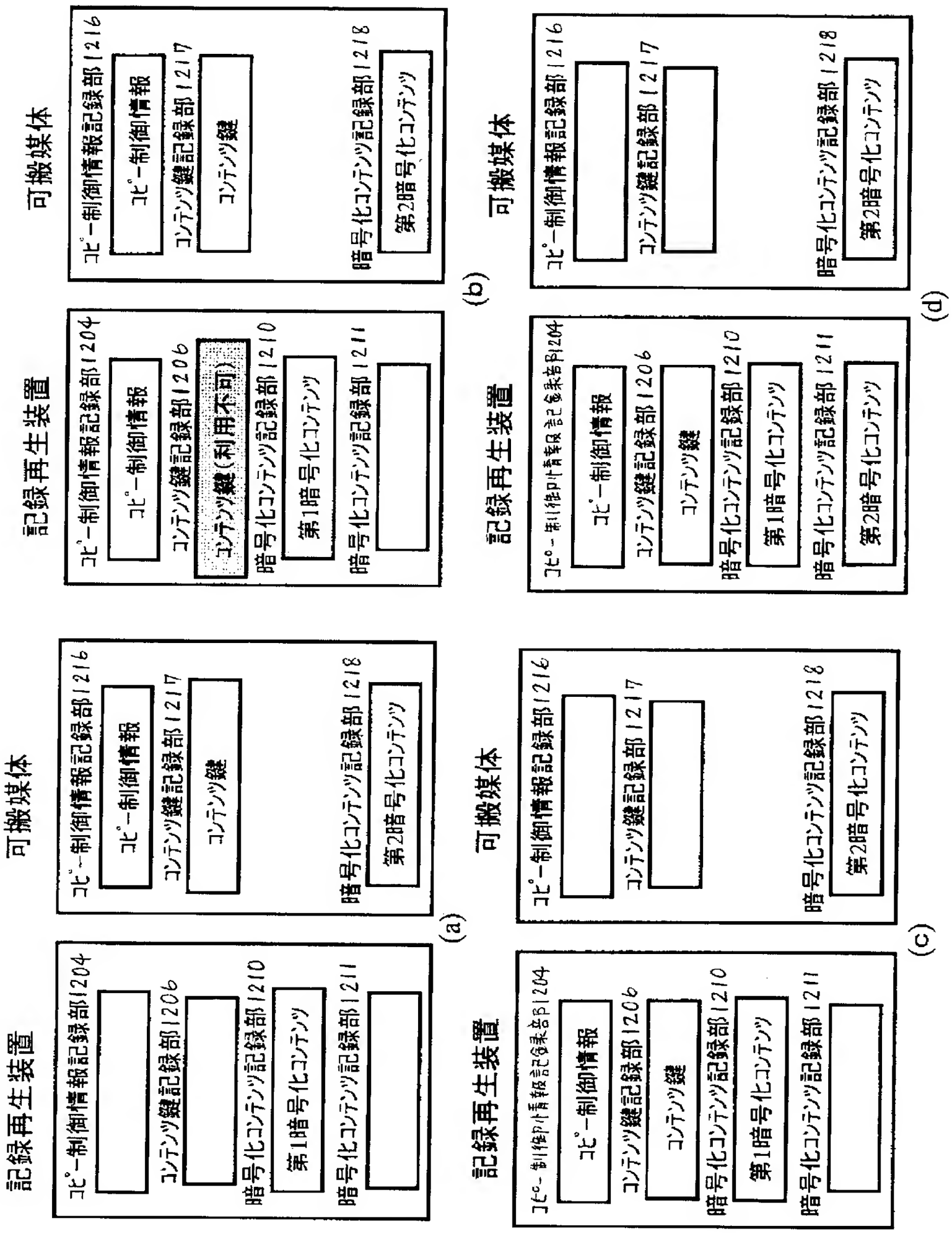
[図32]


可搬媒体
コピー制御情報記録部1216
コピー制御情報
コンテンツ鍵記録部1217
コンテンツ鍵
暗号化コンテンツ記録部1211
第2暗号化コンテンツ
(f)
記録再生装置
コピー制御情報記録部1214
コンテンツ鍵記録部1206
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
(e)
可搬媒体
コピー制御情報記録部1216
コピー制御情報
コンテンツ鍵記録部1217
コンテンツ鍵
暗号化コンテンツ記録部1218
第2暗号化コンテンツ
記録再生装置
コピー制御情報記録部1214
コンテンツ鍵記録部1206
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
第2暗号化コンテンツ
(d)

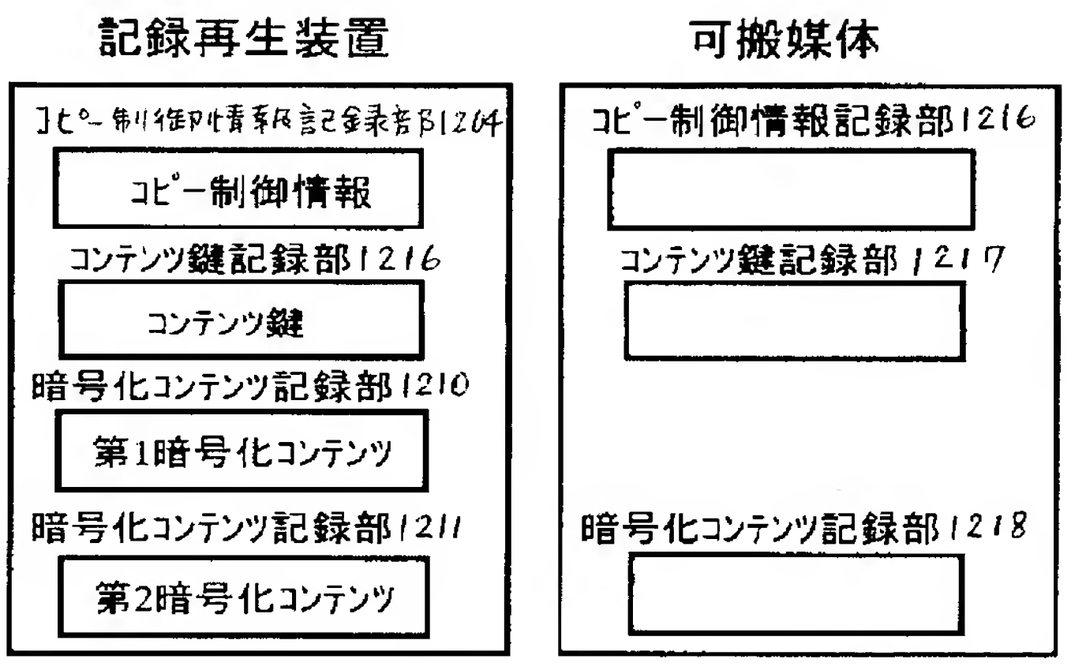
[図33]


START
S601
コピー制御情報判定
NO
END
YES
S602
相互認証
NO
END
YES
S603
可搬媒体からコピー制御情報とコンテンツ鍵を読出す
S604
コピー制御情報とコンテンツ鍵を記録再生装置に記録する(コンテンツ鍵を利用不可状態にする)
S605
可搬媒体のコピー制御情報記録部に記録しているコピー制御情報と、
コンテンツ鍵記録部に記録しているコンテンツ鍵を消去する
(記録再生装置のコンテンツ鍵を利用可能状態にする)
S606
可搬媒体の暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S607
第2暗号化コンテンツを記録再生装置に記録する
S608
可搬媒体の暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

[図34]

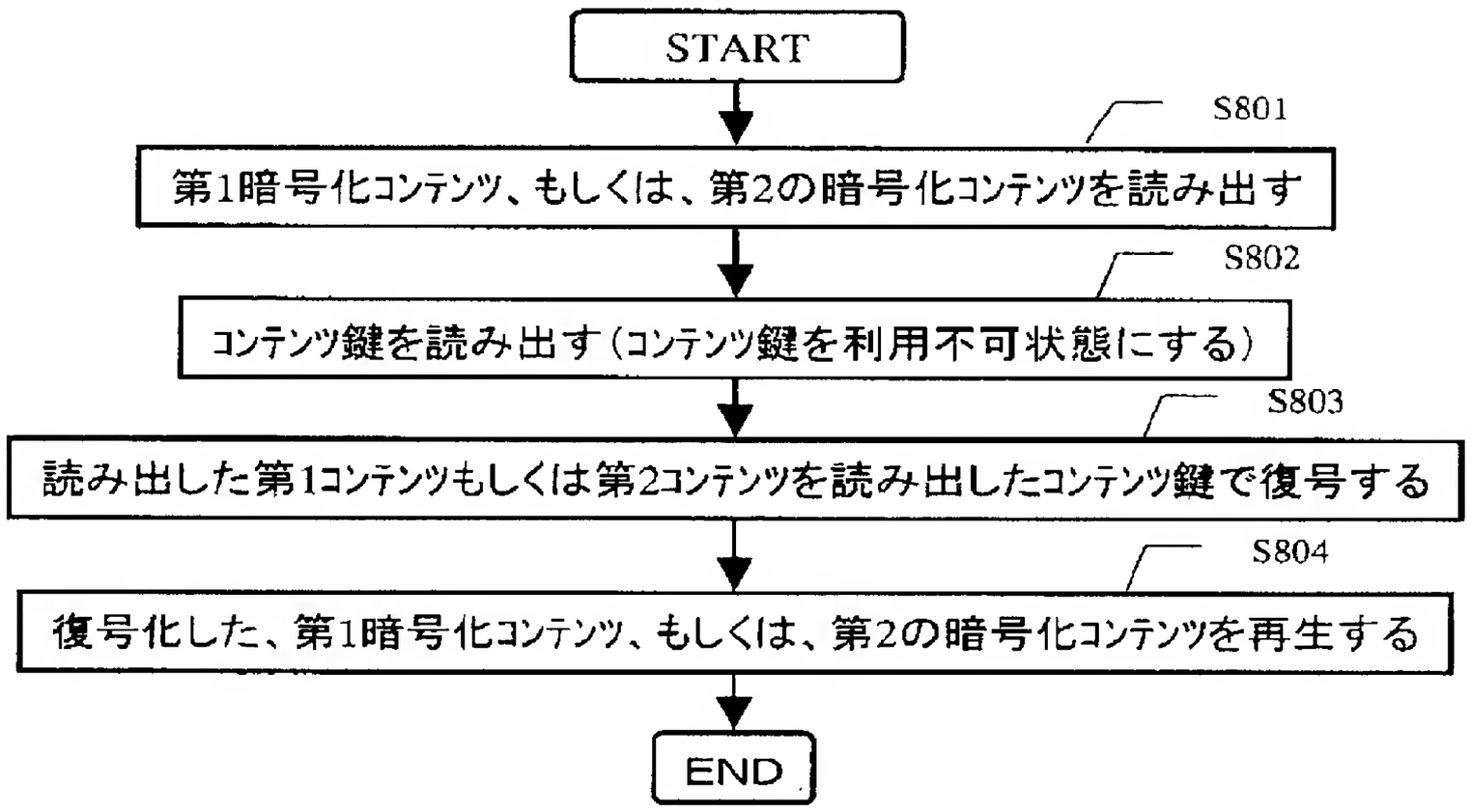

可搬媒体
コピー制御情報記録部1216
コピー制御情報
コンテンツ鍵記録部1217
コンテンツ鍵
暗号化コンテンツ記録部1218
第2暗号化コンテンツ
(a)
記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1206
コンテンツ鍵(利用不可)
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
(b)
可搬媒体
コピー制御情報記録部1216
コンテンツ鍵記録部1217
暗号化コンテンツ記録部1218
第2暗号化コンテンツ
(c)
記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1206
コンテンツ鍵
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
第2暗号化コンテンツ
(d)

[図35]

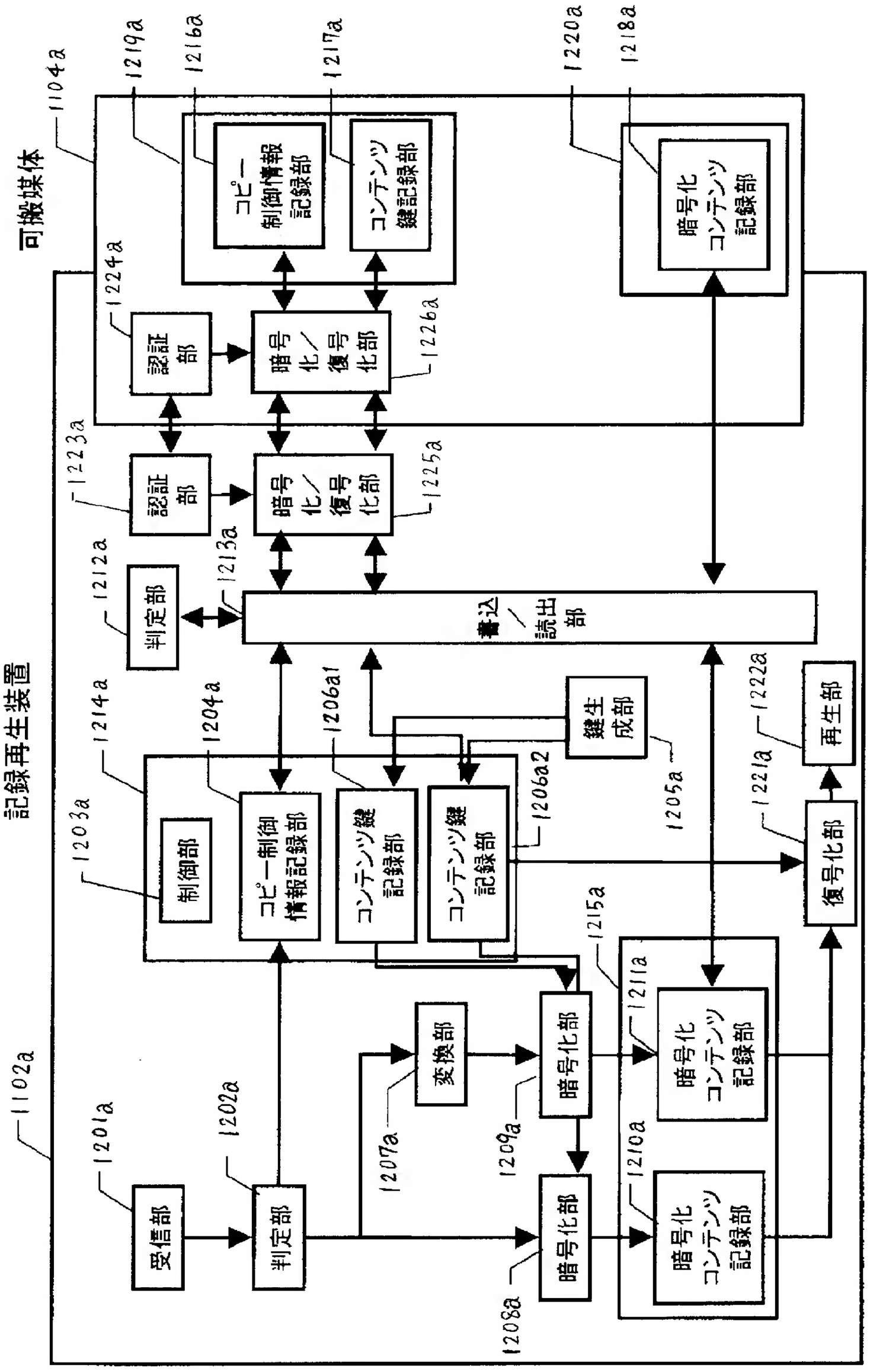

記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1216
コンテンツ鍵
暗号化コンテンツ記録部1210
第1暗号化コンテンツ
暗号化コンテンツ記録部1211
第2暗号化コンテンツ
可搬媒体
コピー制御情報記録部1216
コンテンツ鍵記録部1217
暗号化コンテンツ記録部1218

(e)

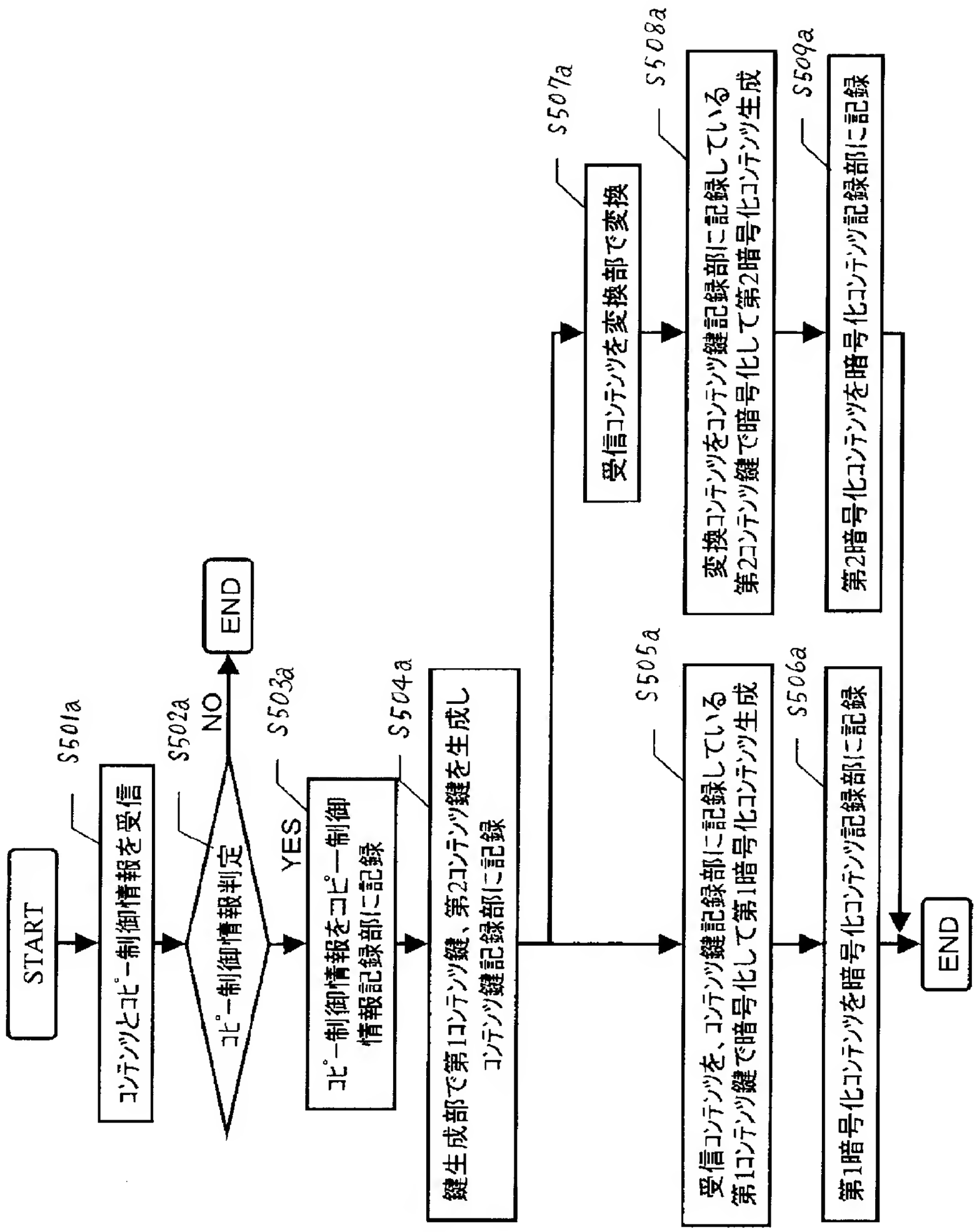
[図36]


START
S801
第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを読み出す
S802
コンテンツ鍵を読み出す(コンテンツ鍵を利用不可状態にする)
S803
読み出した第1コンテンツもしくは第2コンテンツを読み出したコンテンツ鍵で復号する
S804
復号化した、第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを再生する
END

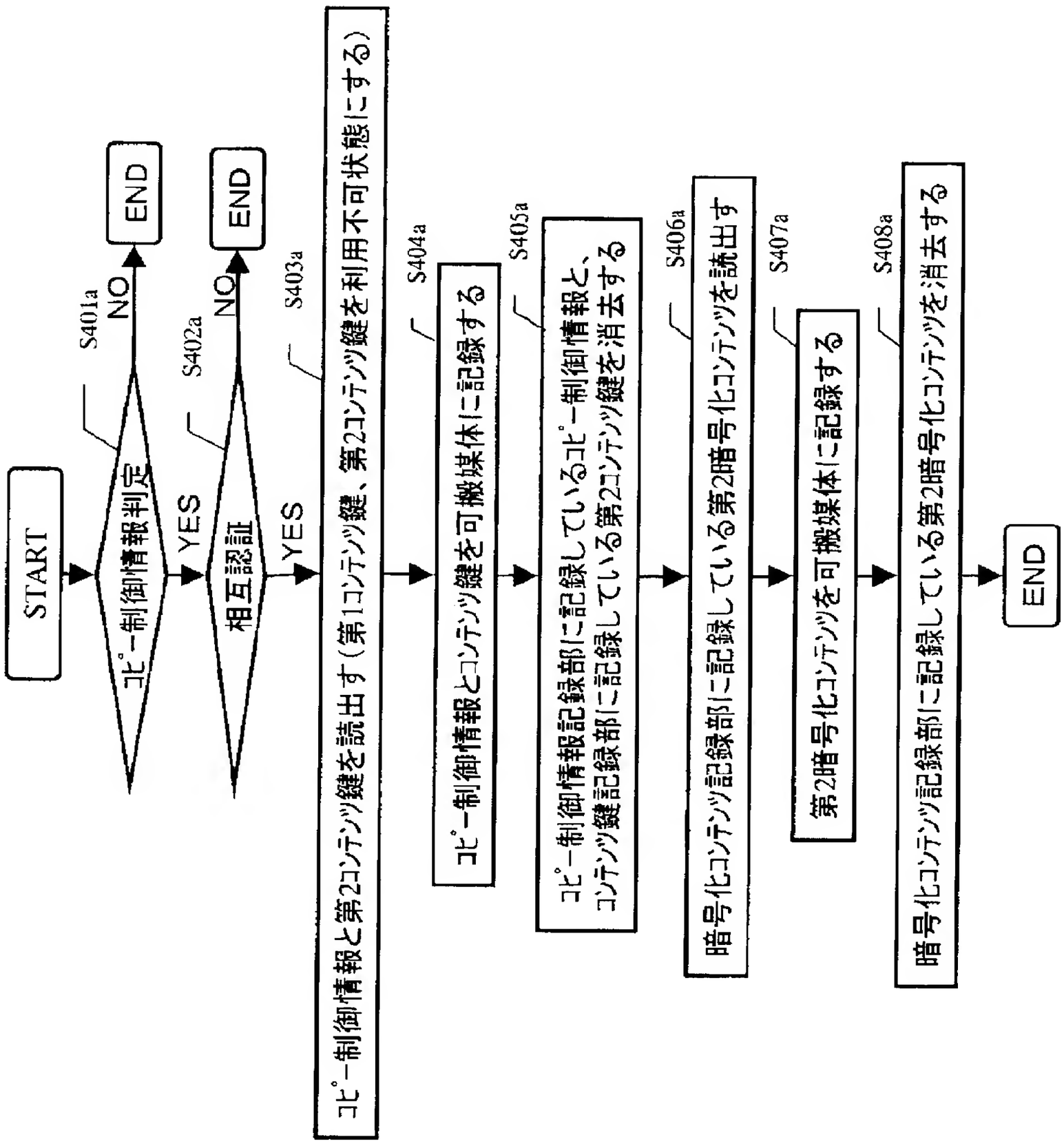
[図37]


記録再生装置
可搬媒体
1102a
1104a
1219a
1216a
1217a
1220a
1218a
コピー制御情報記録部
コンテンツ鍵記録部
暗号化コンテンツ記録部
1224a
認証部
暗号化／復号化部
1226a
1223a
認証部
暗号化／復号化部
1225a
1212a
判定部
1213a
書込／読出部
1214a
1204a
1206a1
鍵生成部
1206a2
1205a
1222a
再生部
1221a
復号化部
1203a
制御部
コピー制御情報記録部
コンテンツ鍵記録部
コンテンツ鍵記録部
1215a
1211a
暗号化コンテンツ記録部
1201a
受信部
1202a
判定部
1207a
変換部
1209a
暗号化部
1210a
暗号化コンテンツ記録部
1208a
暗号化部

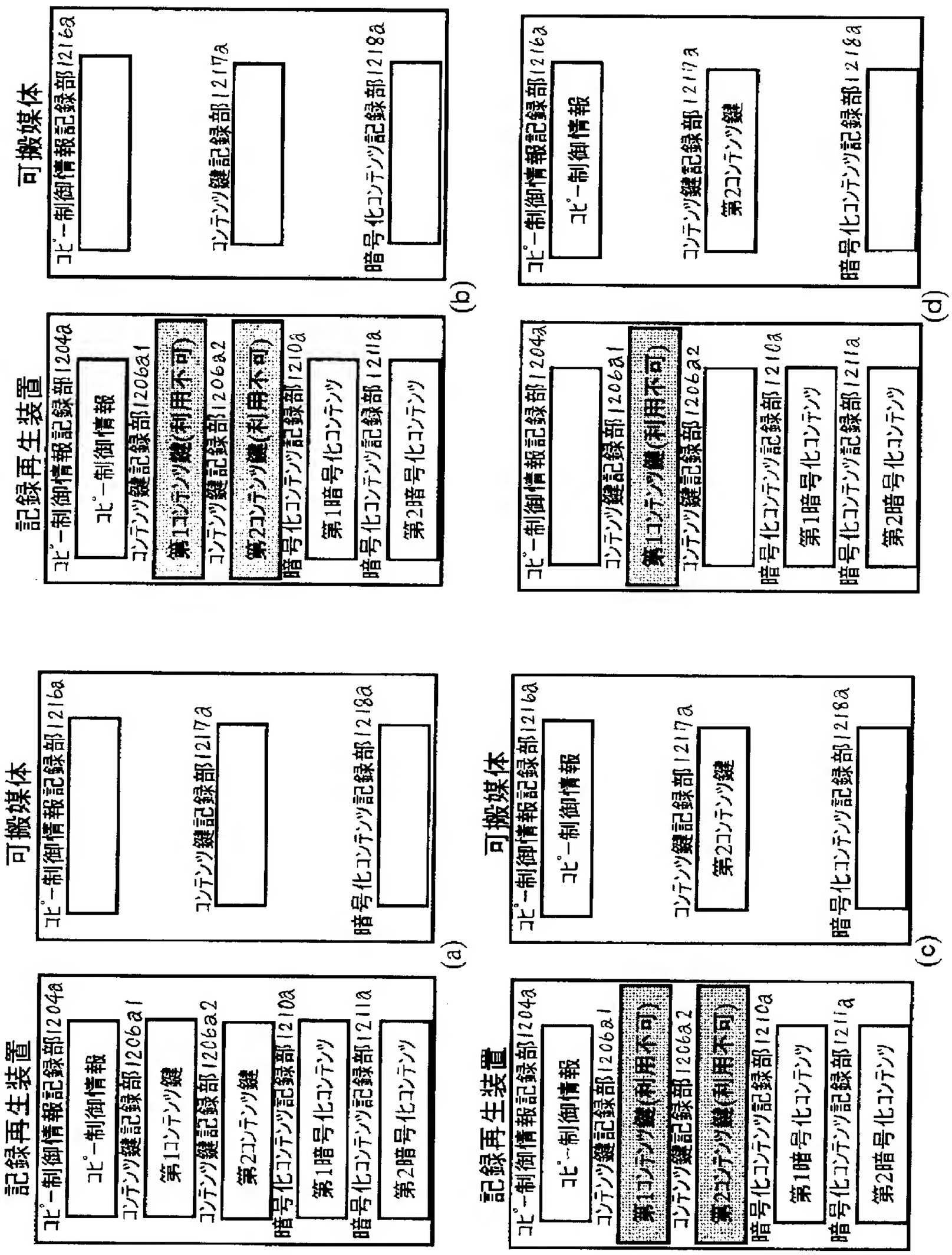
[図38]


START
S501a
コンテンツとコピー制御情報を受信
S502a
コピー制御情報判定
NO
END
YES
S503a
コピー制御情報をコピー制御情報記録部に記録
S504a
コンテンツ鍵生成部で第1コンテンツ鍵、第2コンテンツ鍵を生成し
コンテンツ鍵記録部に記録
受信コンテンツを変換部で変換
S505a
受信コンテンツを、コンテンツ鍵記録部に記録している第1コンテンツ鍵で暗号化して第1暗号化コンテンツ生成
S506a
第1暗号化コンテンツを暗号化コンテンツ記録部に記録
S507a
変換コンテンツをコンテンツ鍵記録部に記録している第2コンテンツ鍵で暗号化して第2暗号化コンテンツ生成
S508a
第2暗号化コンテンツを暗号化コンテンツ記録部に記録
S509a
END

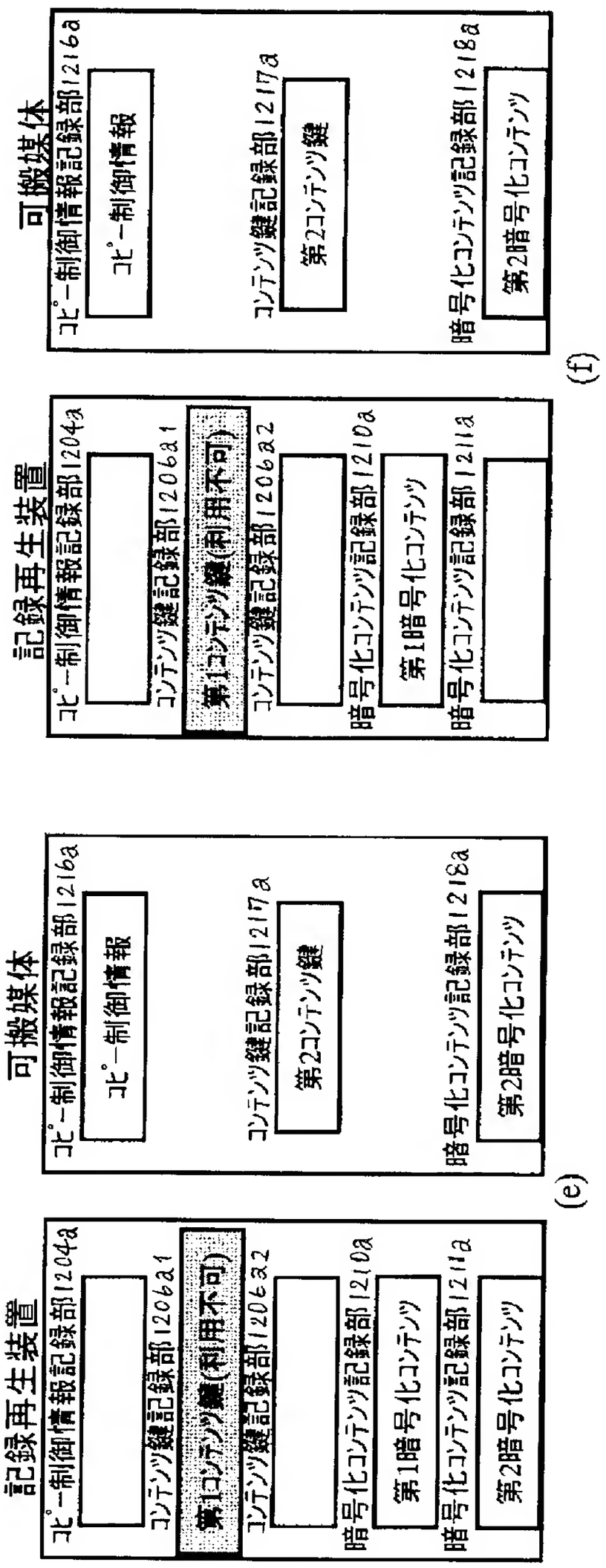
[図39]


START
コピー制御情報判定
S401a
NO
END
YES
相互認証
S402a
NO
END
YES
S403a
コピー制御情報と第2コンテンツ鍵を読出す（第1コンテンツ鍵、第2コンテンツ鍵を利用不可状態にする）
S404a
コピー制御情報とコンテンツ鍵を可搬媒体に記録する
S405a
コピー制御情報記録部に記録しているコピー制御情報と、
コンテンツ鍵記録部に記録している第2コンテンツ鍵を消去する
S406a
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S407a
第2暗号化コンテンツを可搬媒体に記録する
S408a
暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

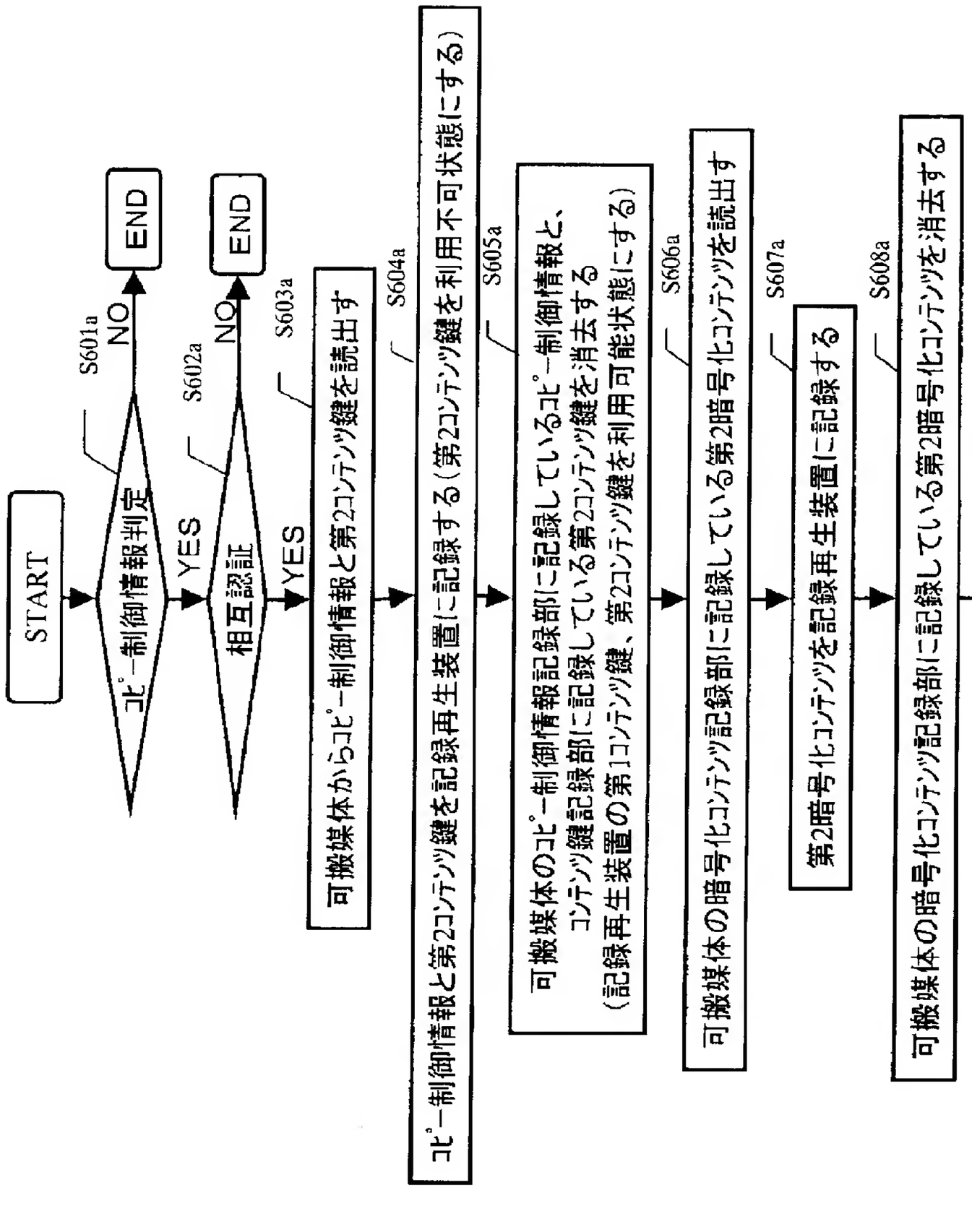
[図40]


可搬媒体
コピー制御情報記録部1216a
コンテンツ鍵記録部1217a
暗号化コンテンツ記録部1218a
(a)
記録再生装置
コピー制御情報記録部1204a
コピー制御情報
コンテンツ鍵記録部1206a1
第1コンテンツ鍵(利用不可)
コンテンツ鍵記録部1206a2
第2コンテンツ鍵(利用不可)
暗号化コンテンツ記録部1210a
第1暗号化コンテンツ
暗号化コンテンツ記録部1211a
第2暗号化コンテンツ
(b)
可搬媒体
コピー制御情報記録部1216a
コピー制御情報
コンテンツ鍵記録部1217a
第2コンテンツ鍵
暗号化コンテンツ記録部1218a
(c)
記録再生装置
コピー制御情報記録部1204a
コンテンツ鍵記録部1206a1
コンテンツ鍵記録部1206a2
暗号化コンテンツ記録部1210a
第1暗号化コンテンツ
暗号化コンテンツ記録部1211a
第2暗号化コンテンツ
(d)

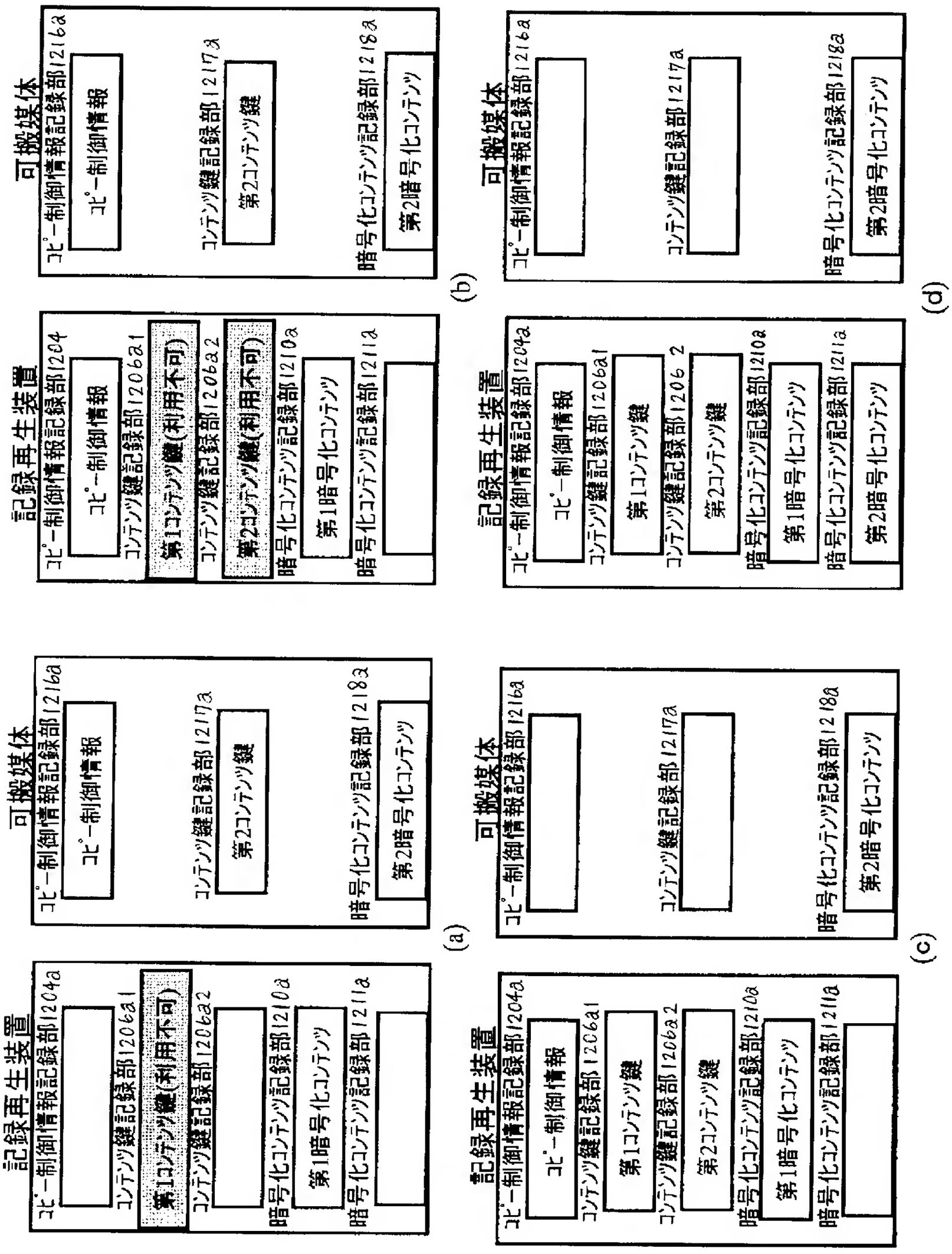
[図41]


(e)
可搬媒体
ｺﾋﾟｰ制御情報記録部1216a
ｺﾋﾟｰ制御情報
ｺﾝﾃﾝﾂ鍵記録部1217a
第2ｺﾝﾃﾝﾂ鍵
暗号化ｺﾝﾃﾝﾂ記録部1218a
第2暗号化ｺﾝﾃﾝﾂ
記録再生装置
ｺﾋﾟｰ制御情報記録部1204a
ｺﾝﾃﾝﾂ鍵記録部1206a1
第1ｺﾝﾃﾝﾂ鍵(利用不可)
ｺﾝﾃﾝﾂ鍵記録部1206a2
暗号化ｺﾝﾃﾝﾂ記録部1210a
第1暗号化ｺﾝﾃﾝﾂ
暗号化ｺﾝﾃﾝﾂ記録部1211a
(f)
可搬媒体
ｺﾋﾟｰ制御情報記録部1216a
ｺﾋﾟｰ制御情報
ｺﾝﾃﾝﾂ鍵記録部1217a
第2ｺﾝﾃﾝﾂ鍵
暗号化ｺﾝﾃﾝﾂ記録部1218a
第2暗号化ｺﾝﾃﾝﾂ
記録再生装置
ｺﾋﾟｰ制御情報記録部1204a
ｺﾝﾃﾝﾂ鍵記録部1206a1
第1ｺﾝﾃﾝﾂ鍵(利用不可)
ｺﾝﾃﾝﾂ鍵記録部1206a2
暗号化ｺﾝﾃﾝﾂ記録部1210a
第1暗号化ｺﾝﾃﾝﾂ
暗号化ｺﾝﾃﾝﾂ記録部1211a

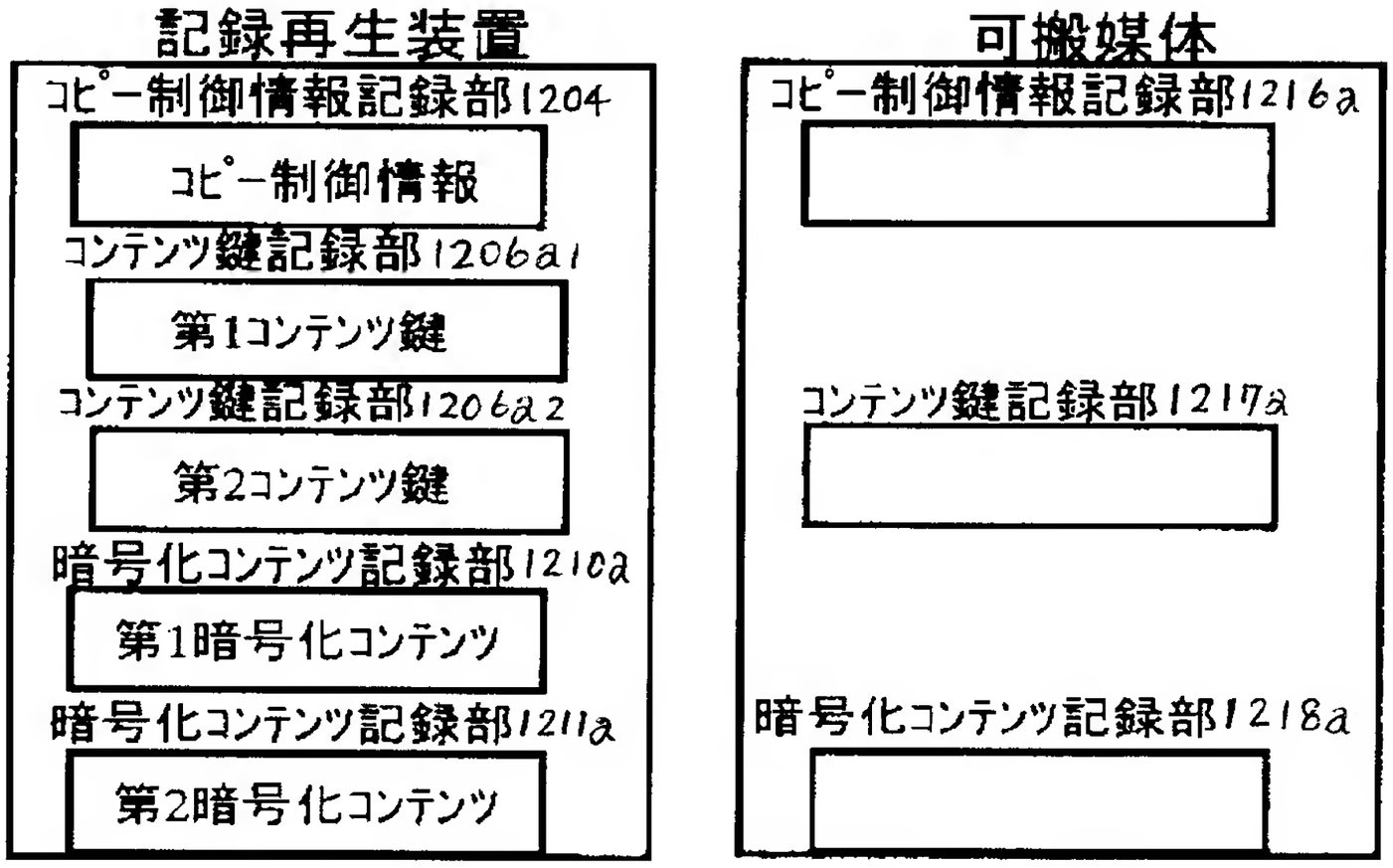
[図42]


START
コピー制御情報判定
S601a
NO
END
YES
S602a
相互認証
NO
END
YES
S603a
可搬媒体からコピー制御情報と第2コンテンツ鍵を読出す
S604a
コピー制御情報と第2コンテンツ鍵を記録再生装置に記録する(第2コンテンツ鍵を利用不可状態にする)
S605a
可搬媒体のコピー制御情報記録部に記録しているコピー制御情報と、
コンテンツ鍵記録部に記録している第2コンテンツ鍵を消去する
(記録再生装置の第1コンテンツ鍵、第2コンテンツ鍵を利用可能状態にする)
S606a
可搬媒体の暗号化コンテンツ記録部に記録している第2暗号化コンテンツを読出す
S607a
第2暗号化コンテンツを記録再生装置に記録する
S608a
可搬媒体の暗号化コンテンツ記録部に記録している第2暗号化コンテンツを消去する
END

[図43]

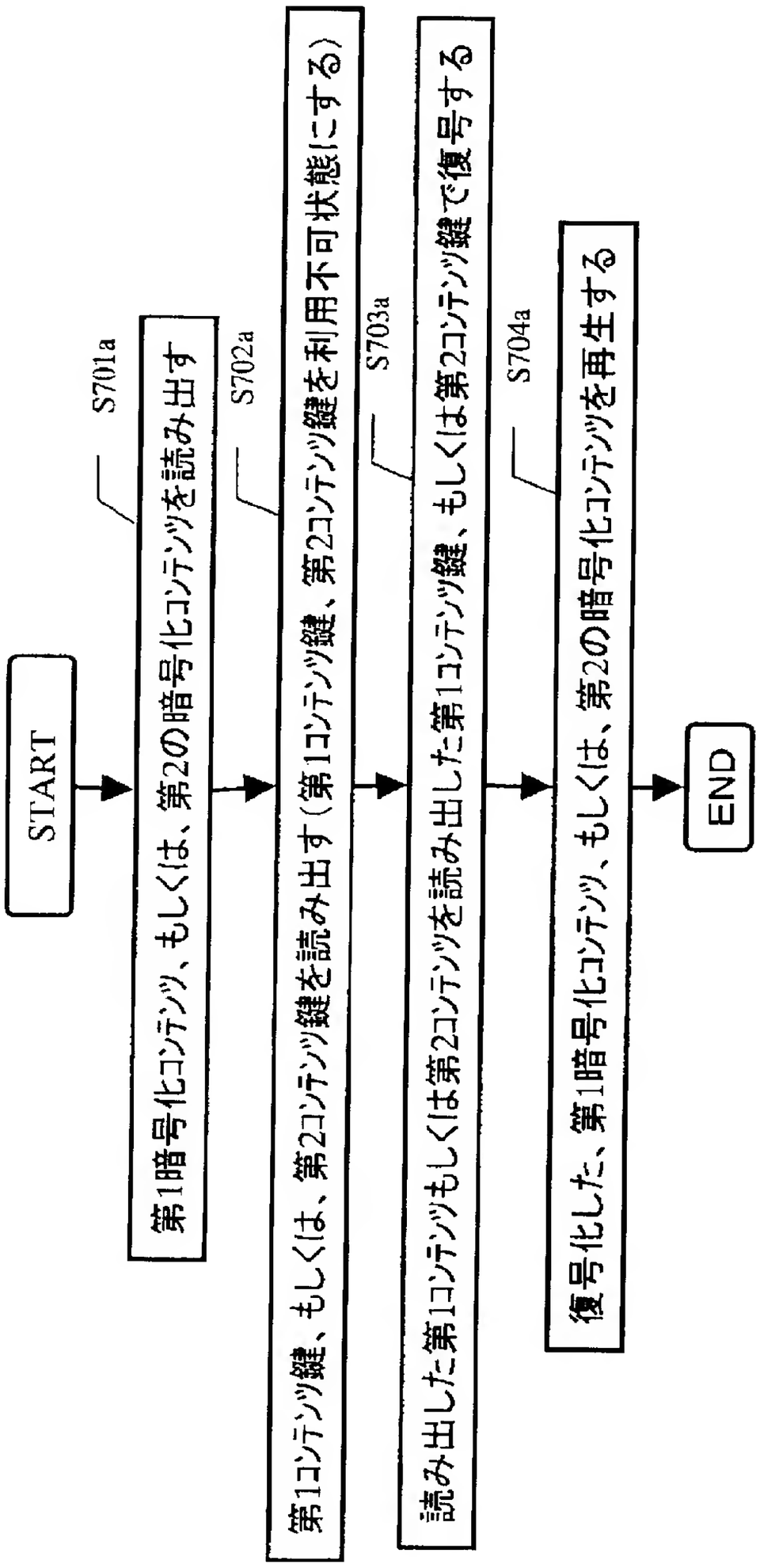

可搬媒体
コピー制御情報記録部1216a
コピー制御情報
コンテンツ鍵記録部1217a
第2コンテンツ鍵
暗号化コンテンツ記録部1218a
第2暗号化コンテンツ
(a)
記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1206a1
第1コンテンツ鍵(利用不可)
コンテンツ鍵記録部1206a2
第2コンテンツ鍵(利用不可)
暗号化コンテンツ記録部1210a
第1暗号化コンテンツ
暗号化コンテンツ記録部1211a
(b)
可搬媒体
コピー制御情報記録部1216a
コンテンツ鍵記録部1217a
暗号化コンテンツ記録部1218a
第2暗号化コンテンツ
(c)
記録再生装置
コピー制御情報記録部1204a
コピー制御情報
コンテンツ鍵記録部1206a1
第1コンテンツ鍵
コンテンツ鍵記録部1206a2
第2コンテンツ鍵
暗号化コンテンツ記録部1210a
第1暗号化コンテンツ
暗号化コンテンツ記録部1211a
(d)

[図44]


記録再生装置
コピー制御情報記録部1204
コピー制御情報
コンテンツ鍵記録部1206a1
第1コンテンツ鍵
コンテンツ鍵記録部1206a2
第2コンテンツ鍵
暗号化コンテンツ記録部1210a
第1暗号化コンテンツ
暗号化コンテンツ記録部1211a
第2暗号化コンテンツ
可搬媒体
コピー制御情報記録部1216a
コンテンツ鍵記録部1217a
暗号化コンテンツ記録部1218a

(e)

[図45]


START
S701a
第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを読み出す
S702a
第1コンテンツ鍵を読み出す（第2コンテンツ鍵を利用不可状態にする）
S703a
読み出した第1コンテンツもしくは第2コンテンツを読み出した第1コンテンツ鍵、第2コンテンツ鍵、もしくは第2コンテンツ鍵で復号する
S704a
復号化した、第1暗号化コンテンツ、もしくは、第2の暗号化コンテンツを再生する
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001398

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06K17/00, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06K17/00, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-347946 A (Deutsche Thomson Brandt GmbH.), 15 December, 2000 (15.12.00), Par. Nos. [0009] to [0010], [0015] to [0017] & EP 1045388 A1 Par. Nos. [0009] to [0010], [0015] to [0017]	1-21
A	JP 2000-207835 A (Matsushita Electric Industrial Co., Ltd.), 28 July, 2000 (28.07.00), Par. No. [0031] & WO 2000/028539 A1 & EP 1001419 A1	1-21

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 28 February, 2005 (28.02.05)	Date of mailing of the international search report 15 March, 2005 (15.03.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001398

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-330871 A (Victor Company Of Japan, Ltd.), 30 November, 2000 (30.11.00), Full text & EP 1054398 A2	1-21
A	JP 11-328033 A (Fujitsu Ltd.), 30 November, 1999 (30.11.99), Full text & US 2001/0032088 A1	1-21

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２００５／００１３９８

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０６Ｆ１２／１４，Ｇ０６Ｋ１７／００，Ｇ０９Ｃ１／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｇ０６Ｆ１２／１４，Ｇ０６Ｋ１７／００，Ｇ０９Ｃ１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000-347946 A（ドイチェ　トムソンーブラント　ゲーエム　ベーハー）2000.12.15，段落【0009】-【0010】，【0015】-【0017】& EP 1045388 A1, pars.[0009]-[0010],[0015]-[0017]	１－２１
A	JP 2000-207835 A（松下電器産業株式会社）　2000.07.28，段落【0031】　& WO 2000/028539 A1 & EP 1001419 A1	１－２１
A	JP 2000-330871 A（日本ビクター株式会社）　2000.11.30，全文　& EP 1054398 A2	１－２１

☒　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２８．０２．２００５	15.3.2005

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	平井　誠	５Ｎ	９０７１
	電話番号　０３－３５８１－１１０１　内線　３５８５		

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２００５／００１３９８

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 11-328033 A（富士通株式会社）　1999.11.30,　全文 & US 2001/0032088 A1	１－２１